MN128-SOHO

IB3

活用ガイド～初級編

■商標についてのお知らせ

◎ Microsoft®、Windows® は、米国Microsoft® Corporationの登録商標です。
◎ Macintosh®、Mac®、MacOS® は、アップルコンピュータ社の登録商標です。
◎ Ethernet® は、富士ゼロックス社の登録商標です。
◎ Super G™は、Atheros Communications, Inc.の商標です。
◎ Adobe、Acrobat、Readerは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における登録商標または商標です。
◎ MN128SOHO™は、株式会社エヌ・ティ・ティ エムイーの商標です。
◎ AutoBACP™、AutoDNS™、AutoMP™、AutoNAT™、AutoPAD™、AutoPPP™、マルチアンサー™は、株式会社ビー・ユー・ジーの商標です。
◎ その他の商品名、会社名は、各社の商標または登録商標です。

■ご注意

・この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。取扱説明書に従って正しい取り扱いをしてください。
・本製品の故障、誤動作、不具合あるいは停電などの外的要因によって、通信などの機会を逃したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。
・通信不良によって生じた損害につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。また、通信内容の漏れにつきましても、当社は一切その責任を負いかねますので、あらかじめご了承ください。
・このマニュアルの著作権は、すべて株式会社エヌ・ティ・ティ エムイーに帰属します。
・このマニュアルの内容の一部または全部を無断で転用することは禁止されています。
・このマニュアルおよびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

もくじ

1 ブロードバンドでインターネットにアクセス

PPPoE接続 ……………………………4
PPPoEセッションキープアライブを使う ‥8
PPPoEセッションキープアライブの
　バックアップ機能を使う …………11

2 ISDNでインターネットにアクセス

パソコン1台で
　インターネット接続（128Kbps）…14
パソコン3台でインターネット接続……17
OCNエコノミー接続する ……………19

3 接続する

手動で接続する ………………………23
自動接続する …………………………26
指定時間内だけ自動接続する…………29
時間によって自動接続する
　プロバイダを変更する ……………32
一定通信料金を超えたら
　自動接続しない……………………36
一定回数を超えたら自動接続しない ……39
自動接続制限状況を見る
　/制限を解除する …………………41

4 切断する

手動で切断する ………………………44
一定時間通信しないとき自動切断する …46
指定時間内だけ
　自動切断するまでの時間を変更する …49
指定時間内だけ自動切断しない ………52

5 通信時間

1回の接続で通信できる時間を制限する…55

6 メール着信通知

メール着信通知機能について …………57
指定した時間間隔で
　メールの着信を確認する …………58
指定した時刻に
　メールの着信を確認する …………62
手動ですぐにメールの着信を確認する …65
特定のメールだけ確認する（フィルタ）…66
着信したメールを設定ページで見る ……69
着信したメールを消去する ……………71

7 メール転送

着信したメールを転送する ……………72
転送できたかどうか確認する …………74

8 Messengerを使う

Windows Messenger、
　MSN Messengerを使う …………75

9 リソースBOD機能を使う

通信中に電話の発信
　着信ができるようにする …………79

10 保守

時刻を設定/修正する …………………81
ユーザIDとパスワードを設定する ……84
接続状況を確認する …………………86
接続/切断ログを見る・消去する ………89
通信料金情報を見る/消去する …………92
1ヶ月ごとの通信料金情報を見る………95
本製品のIPアドレスを確認する ………96
設定を確認する ………………………97
設定をファイルに保存する
　/保存した設定を書き込む …………98
設定を購入時の状態に戻す……………100
本製品のファームウェアの
　バージョンを確認する ……………101
本製品をバージョンアップする………102
本製品を再起動する…………………105

付録

困ったときは…………………………108
設定ページのエラー一覧……………124
クイック設定で
　自動的に設定されるフィルタ ……131
お問い合わせ先………………………138
用語解説………………………………140
索引……………………………………145

活用ガイド

初級編

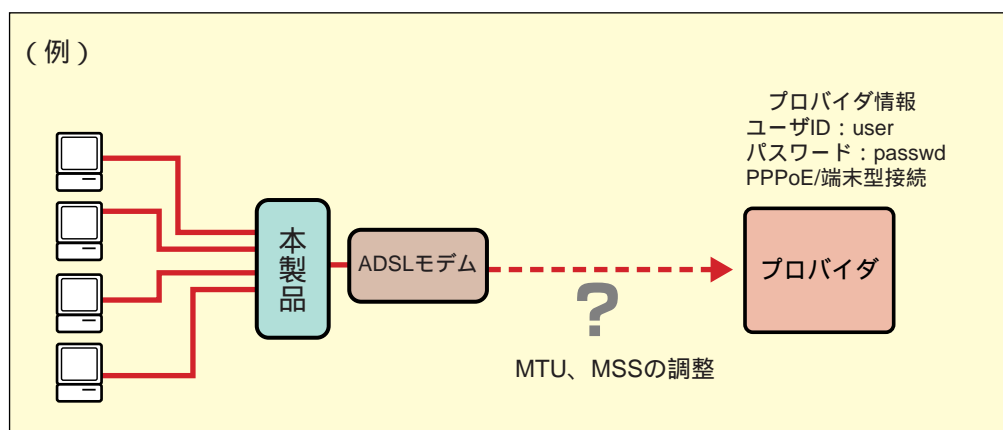
活用ガイド～初級編では、インターネットを使用する上でよく使用する機能や、便利な機能をまとめています。なお、このマニュアルは、事前に「導入/設定ガイド」をお読みになりインターネットにアクセスできることを前提に解説しています。

1. ブロードバンドでインターネットにアクセス ………… 4
2. ISDNでインターネットにアクセス ISDN ………… 14
3. 接続する ………… 23
4. 切断する ………… 44
5. 通信時間 ………… 55
6. メール着信通知 ………… 57
7. メール転送 ………… 72
8. Messengerを使う ………… 75
9. リソースBOD機能を使う ISDN ………… 79
10. 保守 ………… 81

1 ブロードバンドでインターネットにアクセス

ここでは、［詳細設定］メニューの［接続／相手先登録］を使って、ブロードバンドでインターネットにアクセスするための設定を詳しく解説します。

PPPoE接続

PPPoE接続を採用しているプロバイダに接続する設定を詳しく解説します。［クイック設定］→［PPPoE（端末型）］ではうまく接続できない場合の調整方法についても解説しています。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、PPPoEを採用しているプロバイダを登録する番号をクリックします。ここでは、［#8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

2. ［以下の情報を登録する］をクリックします。

3. ［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	PPPoE（ランプ点灯） ※［PPPoE（ランプ点灯）］を選択すると、PPPoE の通信中に、本体前面のPPPoEランプが点灯します。［PPPoE（ランプなし）］は、PPPoEの通信中でもPPPoEランプは点灯しません。両者の違いは、ランプが点灯するかどうかだけです。インターネットに接続するメインのセッションはPPPoEランプを点灯させ、フレッツ・スクウェアなどへのアクセスにはランプを点灯させないなどという使い分けが可能です。
接続モード	端末型接続

［相手先情報］	
相手先名称	プロバイダA
相手先電話番号	
［発信］	
送信ユーザID	user
送信パスワード	••••••
認証プロトコル	相手先に合わせる
DNSサーバアドレス	
通信チャネル	PPPoE(ランプ点灯)
接続モード	端末型接続

プロバイダからPPPoEサービス名、アクセス名の設定を指定されている場合は、［オプション］欄に、次のように入力します。
※特に指定されていない場合は、この設定は不要です。

remote ｛8｝ pppoe sname ｛abc｝
※｛｝の中には、相手先番号を入力します。
※｛abc｝はプロバイダから指定された名前を入力します。

［オプション］

```
remote 8 pppoe sname abc
```

4. 必要に応じて、MSSの値を変更します。

特定のWebサイトが見られない、ネットワークゲームができないなどの問題が起こったときは、MSSの値を変更してみます。

MSS（Maximum Segment Size）とは、TCP接続する際に、1つのTCPパケットで受信できるデータサイズの最大値を、通信相手に通知するために使われるTCPのオプションです。本製品のMSS変換機能を利用すると、パソコンのレジストリを変更しなくても通信が可能になります。初期設定は、「1322」です。
※問題なく動作している場合は、MSSサイズを変更する必要はありません。
※ゲームメーカーやWeb作成者に確認してから、MSSサイズを変更してください。

[MSS設定]	
MSS変換機能	○OFF ◉ON
MSSサイズ	1322

※[MSS変換機能]を[OFF]にすると、変換は行われません。

5. 必要に応じて、MTUの設定を行います。

特定のWebサイトで通信ができなかったり、ゲームなどでのデータの受信が異常に遅いときに、MTUの値を変更します。
MTU（Max Transfer Unit）とは、1回の転送で送信できるパケットの最大値を決める値のことです。MTUサイズが大きいほど一度に多くのデータを送れますが、MTUサイズを大きくしてしまうと、例えば、通信品質があまり良くなくパケットの損失が発生してしまうような回線では、再送の発生により転送効率が悪くなりかえって通信速度が遅くなるという結果になることがあります。「1454」などの値を入力してください。
※問題なく動作している場合は、MTUの設定を行う必要はありません。設定を行わない場合、PPPoE接続では「1492」が使用されます（PPPoE以外の接続では1500が使用されます）。

[MTU設定]	
MTUサイズ	1454

6. [実行]ボタンをクリックします。

プロバイダに関する設定が終了しました。
実際にプロバイダに接続する方法は、「手動で接続する」〈P.23〉を参照してください。どれか1台のパソコンで接続の操作を行うと、どのパソコンでもインターネットにアクセスできます。

なお、自動的にプロバイダに接続したいときは、「自動接続する」〈P.26〉を参照してください。

7. WAN側からの不正なアクセスするのを防止するため、設定ページにユーザIDとパスワードを設定します。[詳細設定]をクリックし、[管理コマンド・設定]→[ユーザ・パスワード変更]をクリックします。

[管理者コマンド・設定（ユーザ・パスワード変更）]画面が表示されます。

8. 次のように入力します。

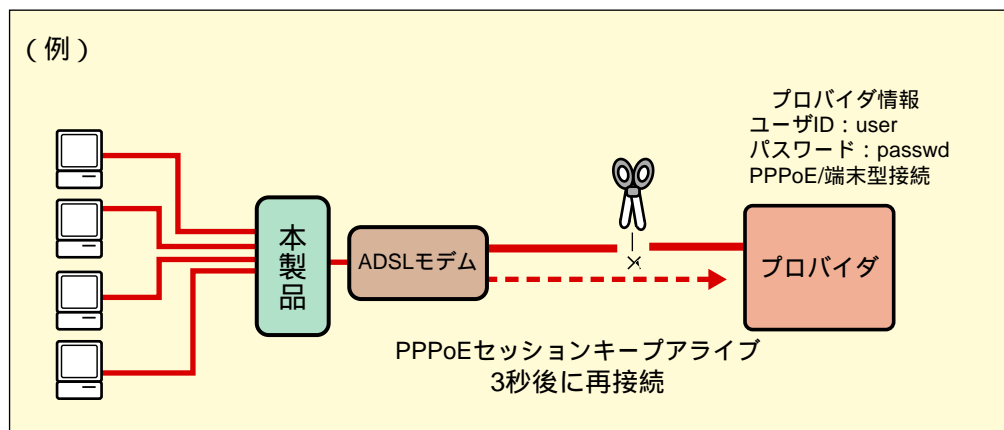
ユーザID	ユーザIDを入力 ※「no」「clear」は使用できません。
パスワード	パスワードを入力 ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
パスワード（再入力）	［パスワード］に入力した文字を入力

9. ［設定］ボタンをクリックします。

以降、管理者が設定ページを開くときは［パスワード要求］ダイアログで上記で設定した［ユーザID］と［パスワード］を入力してください。ユーザIDとパスワードを忘れると、設定ページを開くことができません。ご注意ください。

ADSLまたはFTTHを使用してインターネットに常時接続できる環境では、外部からの不正アクセスや攻撃の被害に遭う危険性も高くなります。本製品のステルスモード、SPI機能、IPフィルタなどを使用して、セキュリティ対策は十分に行ってください。なお、クイック設定を行ったときは、自動的にIPフィルタが設定されます。
ステルスモード、SPI機能、IPフィルタに関しては、活用ガイド〜中・上級編「7.ルータ機能のセキュリティ」を参照してください。

PPPoEセッションキープアライブを使う

PPPoEを採用しているプロバイダでは、メンテナンスなどの都合でプロバイダ側からPPPoE接続を切断される場合があります。PPPoEセッションキープアライブ機能を使用すると、何らかの理由で接続が切断された場合、自動で定期的にプロバイダに再接続を試みます。

PPPoEセッションキープアライブ機能による再接続は、常に接続を保とうとする機能であり、自動接続の設定とは別のものです。ご注意ください。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［＃０］～［＃１５］の中から、PPPoEセッションキープアライブの設定をしたい相手先の番号をクリックします。ここでは、［＃０］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

2. ［以下の情報を登録する］をクリックします。

3. ［発信］の各項目で、次のように設定します。

※すでに設定している接続に、PPPoEセッションキープアライブの設定を行うときは、［発信］の設定を行う必要はありません。

相手先名称	名称（何でも構いません。例：プロバイダA）を設定 ※「no」「clear」は使用できません。
送信ユーザID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
通信チャネル	PPPoE（ランプ点灯） ※［PPPoE（ランプ点灯）］を選択すると、PPPoEの通信中に、本体前面のPPPoEランプが点灯します。［PPPoE（ランプなし）］は、PPPoEの通信中でもPPPoEランプは点灯しません。両者の違いは、ランプが点灯するかどうかだけです。インターネットに接続するメインのセッションはPPPoEランプを点灯させ、フレッツ・スクウェアなどへのアクセスにはランプを点灯させないなどという使い分けが可能です。
接続モード	端末型接続

［相手先情報］	
相手先名称	ﾌﾟﾛﾊﾞｲﾀﾞA
相手先電話番号	
［発信］	
送信ユーザID	user
送信パスワード	••••••
認証プロトコル	相手先に合わせる
DNSサーバアドレス	
通信チャネル	PPPoE(ランプ点灯)
接続モード	端末型接続

4. ［PPPoEセッションキープアライブ設定］の項目の［セッションキープアライブ機能］で［ON］を選択します。

5. ［実行］ボタンをクリックします。

以降、プロバイダから切断されると、約3秒後にプロバイダに再接続を試みます。接続できなかった場合は、接続できるまで再接続を試みます。再接続する間隔は、1分後、2分後、3分後、と1分ずつ増えていき、最大10分後になり、以降10分間隔で再接続を試みます。
なお、再接続を試みている最中に、意図的に発信した場合や、自動接続した場合は、PPPoEセッションキープアライブ機能は停止します。

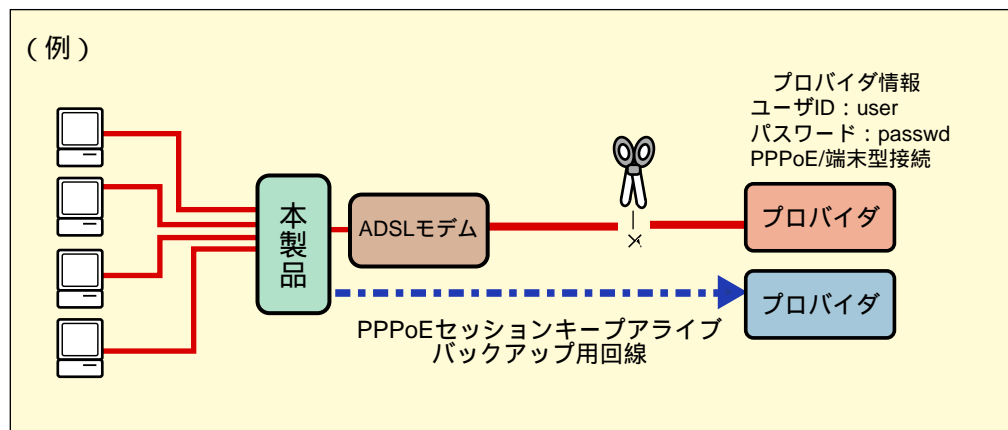
◆PPPoEセッションキープアライブ機能を停止しないようにする

PPPoEセッションキープアライブ拡張機能を使用すると、PPPoEセッションキープアライブ機能を停止しないようにできます。［接続／相手先登録］画面の［オプション］で、次のように入力してください。

remote {0} pppoe always on

※｛｝の中には、相手先番号を入力します。

PPPoEセッションキープアライブのバックアップ機能を使う

PPPoEによるブロードバンド接続を行っているとき、回線の切断に備えてバックアップ回線を設定しておくことができます。何らかの理由で、PPPoEによるブロードバンド接続が切断されたとき、指定されたバックアップ回線に自動的に発信されます。なお、バックアップ回線として設定できるのは、ISDN回線、PHS（PHSカードまたはFOMA PCカード型端末）の回線です。

ISDN/PHS/FOMAをバックアップ回線として使用する場合、通信時間に応じた通信料金がかかります。そのため、バックアップ回線による通信が長時間に渡ると、通信料金も高額になりますので、ご注意ください。

設定ページ

1. バックアップ用の回線の設定を行います。

［詳細設定］をクリックし、［接続／相手先登録］→［＃０］～［＃１５］の中から、バックアップ用の回線としたい相手先番号を設定します。（ここでは、PCカードから発信する場合を例に解説します。PCカードの設定はあらかじめ行っていることとします。）

クリックした番号の［接続／相手先登録］画面が表示されます。

相手先の電話番号、送信ユーザIDなどの設定を行い、［通信チャネル］でPCカードを選択します。

2 ［以下の情報を登録する］をクリックし、［実行］ボタンをクリックします。

ここでいったん回線に接続し、インターネットに接続できることを確認してください。

3. PPPoEセッションキープアライブのバックアップ機能を使用する、PPPoE接続の設定を行います。

［詳細設定］をクリックし、［接続／相手先登録］→［＃０］～［＃１５］の中から、PPPoEセッションキープアライブのバックアップ機能の設定をしたい相手先の番号をクリックします。ここでは、［＃０］をクリックします。

クリックした番号の［接続／相手先登録］画面が表示されます。

4. ［以下の情報を登録する］をクリックします。

5. ［発信］の各項目で、次のように設定します。

※すでに設定している接続に、PPPoEセッションキープアライブの設定を行うときは、［発信］の設定を行う必要はありません。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	PPPoE（ランプ点灯） ※［PPPoE（ランプ点灯）］を選択すると、PPPoE の通信中に、本体前面のPPPoEランプが点灯します。［PPPoE（ランプなし）］は、PPPoEの通信中でもPPPoEランプは点灯しません。両者の違いは、ランプが点灯するかどうかだけです。インターネットに接続するメインのセッションはPPPoEランプを点灯させ、フレッツ・スクウェアなどへのアクセスにはランプを点灯させないなどという使い分けが可能です。
接続モード	端末型接続

6. ［PPPoEセッションキープアライブ設定］の項目の［セッションキープアライブ機能］で［バックアップ］を選択します。

7 ［バックアップ用相手先］を選択します。

※下の画面は、「#8」を選択している場合です。

8 ［設定］ボタンをクリックします。

指定した回線がバックアップ回線として使用されます。
以降、プロバイダから切断されると、自動的にバックアップ回線に切り替わるようになります。いったんバックアップ回線に切り替わった後も、セッションキープアライブ機能が有効になっているため、切断されたブロードバンド回線の再接続が試行されます。
なお、セッションキープアライブ機能により、PPPoE接続が復活したら、ブロードバンド回線に切り替わり、バックアップ回線は自動的に切断されます。

バックアップ回線を指定できるのは、PPPoEによる接続のみです。［接続/相手先登録］画面の［通信チャネル］でPPPoE以外を選択している場合は、バックアップ回線の設定を行っても無効になります。

◇バックアップ回線で自動切断時間が設定されている場合

バックアップ回線の設定で、自動切断時間が設定されているとき、その時間通信が行われなかった場合は、自動的にバックアップ回線が切断されます。

2 ISDNでインターネットにアクセス

ここでは、［詳細設定］メニューの［接続／相手先登録］を使って、ISDNでインターネットにアクセスするための設定を解説します。

パソコン1台でインターネット接続（128Kbps）

本製品のLANポートにパソコンを1台のみ接続し、同期128Kbpsでインターネットに接続したい場合の設定をご紹介します。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、インターネット接続したい相手先の番号をクリックします。ここでは、［#8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

2. ［以下の情報を登録する］をクリックします。

3. ［相手先情報］［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000 ※ 128Kbps　MP に対応したアクセスポイントの番号を入力してください。
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	2B（128Kbps/MP）
接続モード	端末型接続

4. ［実行］ボタンをクリックします。

5. 画面左側の［自動接続相手先］をクリックします。
［自動接続相手先］画面が表示されます。

6. ［自動接続相手先1］と［自動接続相手先2］で、［なし］を選択します。

7. ［設定］ボタンをクリックします。

実際にプロバイダに接続する方法は、「手動で接続する」〈P.23〉を参照してください。

パソコン3台でインターネット接続

本製品のLANポートにパソコンを3台接続しているとき、どのパソコンからでもインターネットを利用する場合の設定をご紹介します。この場合、どれか1台のパソコンが回線をインターネットに接続すれば、ほかのパソコンでは接続の操作をせずにインターネットを利用できます。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、インターネット接続したい相手先の番号をクリックします。ここでは、［#8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

2. ［以下の情報を登録する］をクリックします。

3. ［相手先情報］［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

4. ［実行］ボタンをクリックします。

5. 画面左側の［自動接続相手先］をクリックします。

   ［自動接続相手先］画面が表示されます。

6. ［自動接続相手先1］と［自動接続相手先2］で、［なし］を選択します。

7. ［設定］ボタンをクリックします。

   実際にプロバイダに接続する方法は、「手動で接続する」〈P.23〉を参照してください。どれか1台のパソコンが接続の操作をすると、どのパソコンでもインターネットにアクセスできます。

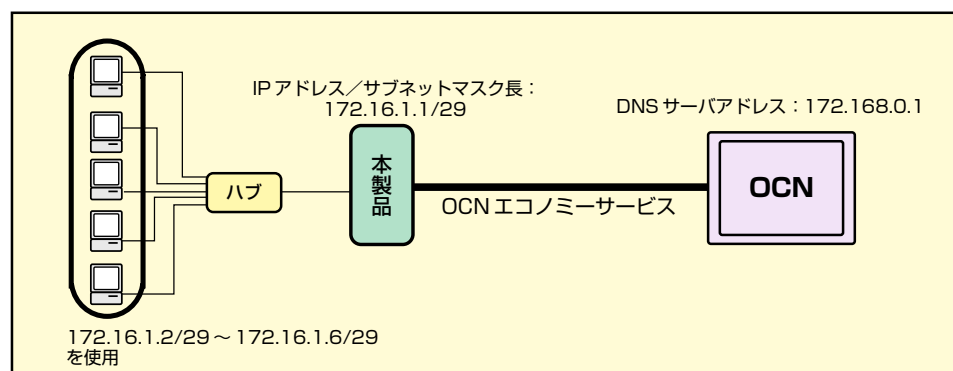
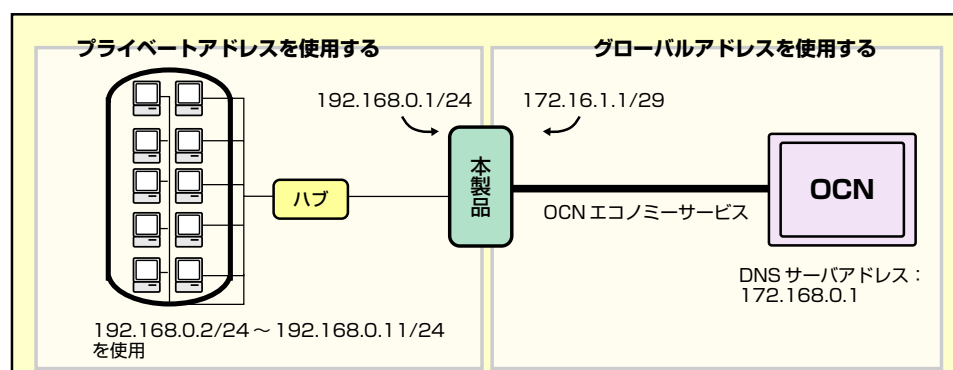
OCNエコノミー接続する

OCNエコノミーサービスを契約すると、グローバルIPアドレスを取得し、常時接続することができます。ここでは次のような契約内容を例に解説します。

OCN側のDNSサーバのIPアドレス/サブネットマスク長：
172.168.0.1/29

取得するIPアドレス/サブネットマスク長：
172.16.1.0/29～172.16.1.7/29（8個）

また、ここでは、次の2つのパターンの設定例について、まとめて解説します。

（例1）LAN内のパソコンにグローバルIPアドレスを割り当てる

（例2）LAN内のパソコンにプライベートIPアドレスを割り当てる

設定ページ

1. 設定ページを開き、クイック設定ページの［ISDNで接続］→［端末型ダイヤルアップ］をクリックします。
   ［ISDNクイック設定（端末型ダイヤルアップ）］画面が表示されます。

2. ［相手先名称］に「OCN」と入力します。

3. ［設定］ボタンをクリックします。確認のメッセージが表示されたら［OK］ボタンをクリックします。

4. 詳細設定ページを開き、［接続/相手先登録］→「#0 OCN」をクリックします。
   ［接続/相手先登録］画面が表示されます。

5. ［発信］で次の項目を設定します。

DNSサーバアドレス	OCNエコノミーで指定されたDNSサーバアドレスを入力
通信チャネル	2B（128Kbps/MP）
接続モード	LAN型接続

6. ［自動切断］で、［最大接続時間］［自動切断タイマ1］をそれぞれ「0」に設定します。

7. ［自動接続制限］で［料金による制限］［接続回数による制限］をそれぞれ「0」に設定します。

[自動接続制限]
料金による制限　0 円／日
接続回数による制限　0 回／分

8. ［以上の情報を登録する］をクリックし、［実行］ボタンをクリックします。確認のメッセージが表示されたら［OK］ボタンをクリックします。

9. 詳細設定ページの［ルータ設定］→［ISDN］をクリックします。
［ルータ設定（ISDN）］画面が表示されます。

10. ［回線種別］で［専用線128kbps］を選択します。

11. ［設定］ボタンをクリックします。確認のメッセージが表示されたら［OK］ボタンをクリックします。

12. 詳細設定ページの［ルータ設定］→［LAN］をクリックします。
［ルータ設定（LAN）］画面で、LAN上の機器に割り当てるIPアドレスを指定します。

(1)　LAN内のIPアドレスにグローバルIPアドレスを使用する場合

［基本］→［本体のIPアドレス/サブネットマスク長］	172.16.1.1/29
［DHCPサーバ］→［開始IPアドレス/個数］	172.16.1.2/5
［オプション］	次のコマンドを入力 ip route 0.0.0.0/0/7 remote 0 static

(2)　LANのIPアドレスにプライベートIPアドレスを使用する場合

[基本] → [本体の IP アドレス / サブネットマスク長]	192.168.0.1/24 のまま
[DHCP サーバ] → [開始 IP アドレス / 個数]	192.168.0.2/10
[オプション]	次のコマンドを入力 ip nat 1 192.168.0.1 172.16.1.1 remote 0 ip nat 2 192.168.0.2 172.16.1.2 remote 0 ip nat 3 192.168.0.3 172.16.1.3 remote 0 ip nat 4 192.168.0.4 172.16.1.4 remote 0 ip nat 5 192.168.0.5 172.16.1.5 remote 0 ip nat 6 192.168.0.6-192.168.0.11 172.16.1.6 remote 0 ip route 0.0.0.0/0/7 remote 0 static

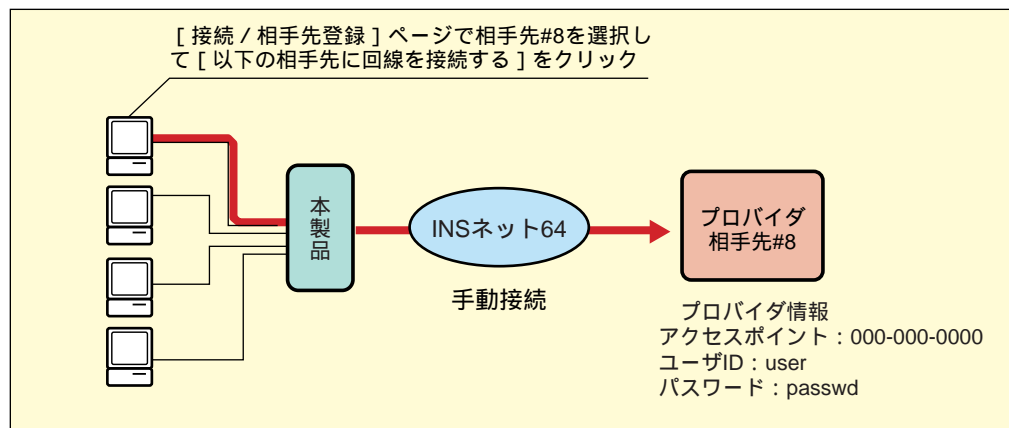
13. [設定] ボタンをクリックします。確認のメッセージが表示されたら [OK] ボタンをクリックします。

14. 回線を接続し、本体およびパソコンを再起動してください。

3 接続する

ここでは、回線を接続する方法について解説しています。時間や通信料金などの条件を設定して、自動接続を制限したり、時間帯によって接続先を切り替えることなどができます。

手動で接続する

手動で回線を接続する方法を解説します。なお、LANポートにつないだほかのパソコンですでに相手先に接続しているときは、その回線を共有することができます。改めて接続する必要はありません。接続の操作を行う前に、現在の接続状況を確認することをお勧めします。→「接続状況を確認する」〈P.86〉

◆ 意図していない接続を行うことがあります。

ネットワークやパソコンの設定内容や運用によっては、回線が接続したままになっていたり、意図していない自動接続を行うことがあります。（例えば、一部のWebサイトではサーバから情報を送り続けるものがあります。）お客様の意図していない接続について、弊社は一切責任を負いかねますので、あらかじめご了承ください。

とくに端末型ダイヤルアップ接続の場合は、本製品の導入後しばらくは、接続の状況や通信料金にご注意ください。接続の状況や通信料金は次の場所で確認することができます。

- 本体のランプ　→　回線接続中、ISDNをお使いの場合はB1またはB2ランプが点灯します。
  ※ブロードバンドの場合は、WANランプやPPPoEランプが点灯します。設定によっては、PPPoEランプは点灯しないことがあります。
- 設定ページの［切断／接続状況］画面→「接続状況を確認する」〈P.86〉
- 設定ページの［情報表示（通信料金）］画面→「通信料金情報を見る／消去する」〈P.92〉

意図しない接続を防ぐために、本製品では各種接続制限機能があります。必要に応じてご利用ください。詳しくは、下記のページを参照してください。

- 「指定時間内だけ自動接続する」〈P.29〉
- 「時間によって自動接続するプロバイダを変更する」〈P.32〉
- 「一定通信料金を超えたら自動接続しない」〈P.36〉

・「一定回数を超えたら自動接続しない」〈P.39〉

また、次の環境では本製品を使用しないように注意してください。

- すでに稼働しているLANに本製品を導入するとき、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行うことは避けてください。
- LANポートにつないだパソコンで、定期的に回線を接続して通信を行うソフトウェアを起動したままにしないでください。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、手動で接続する相手先の番号をクリックします。ここでは、［#8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

接続／相手先登録#8　Help

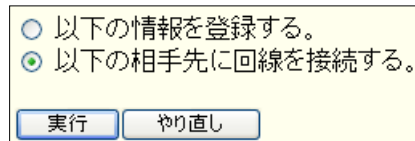
◆相手先の情報を登録したり、相手先に回線を手動で接続します。

Message

パラメータを入力・修正し、操作を選んで［実行］ボタンをクリックしてください。

送信パスワード／受信パスワード／鍵配送鍵は、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

◉ 以下の情報を登録する。
○ 以下の相手先に回線を接続する。

［実行］［やり直し］

［相手先情報］
相手先名称
相手先電話番号
［発信］
送信ユーザID

2. ［発信］の各項目で、次のように設定します。

項目	設定
相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

3. ［以下の相手先に回線を接続する。］をクリックします。

4. ［実行］ボタンをクリックします。

「接続しました。」という内容のメッセージが表示されます。

自動接続する

Webブラウザで見たいホームページのURLを指定したり、メールソフトで送受信の操作を行うと、自動的に回線をつないでインターネットにアクセスできるようにします。

※ブロードバンド、またはフレッツ・ISDNをご利用の場合は、クイック設定でインターネットへアクセスするための設定を行うと、自動接続の設定が有効になっています。

◆ 意図していない接続を行うことがあります。

ネットワークやパソコンの設定内容や運用によっては、回線が接続したままになっていたり、意図していない自動接続を行うことがあります。（例えば、一部のWebサイトではサーバから情報を送り続けるものがあります。）お客様の意図していない接続について、弊社は一切責任を負いかねますので、あらかじめご了承ください。

とくに端末型ダイヤルアップ接続の場合は、本製品の導入後しばらくは、接続の状況や通信料金にご注意ください。接続の状況や通信料金は次の場所で確認することができます。

- 本体のランプ　→　回線接続中は、ISDNをご利用の場合はB1またはB2ランプが点灯します。
  ※ブロードバンドの場合は、WANランプやPPPoEランプが点灯します。設定によっては、PPPoEランプは点灯しないことがあります。
- 設定ページの［切断／接続状況］画面→「接続状況を確認する」〈P.86〉
- 設定ページの［情報表示（通信料金）］画面→「通信料金情報を見る／消去する」〈P.92〉

意図しない接続を防ぐために、本製品では各種接続制限機能があります。必要に応じてご利用ください。詳しくは、下記のページを参照してください。

- 「指定時間内だけ自動接続する」〈P.29〉
- 「時間によって自動接続するプロバイダを変更する」〈P.32〉
- 「一定通信料金を超えたら自動接続しない」〈P.36〉
- 「一定回数を超えたら自動接続しない」〈P.39〉

また、次の環境では本製品を使用しないように注意してください。

- すでに稼働しているLANに本製品を導入するとき、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行うことは避けてください。
- LANポートにつないだパソコンで、定期的に回線を接続して通信を行うソフトウェアを起動したままにしないでください。

◆Windowsの「インターネット接続共有サービス」を利用しているとき
意図していない自動接続を行うことがあります。その際の料金トラブルについては、弊社は一切責任を負いかねますので、あらかじめご了承ください。

設定ページ

1. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、自動接続する相手先の番号をクリックします。ここでは、［#8］をクリックします。
   クリックした番号の［接続／相手先登録］画面が表示されます。

2. ［以下の情報を登録する］をクリックします。

3. ［相手先情報］［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダA）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

4. ［実行］ボタンをクリックします。

5. 画面左側の［自動接続相手先］をクリックします。

6. ［自動接続相手先1］から自動接続したい相手先を選択します。

※自動接続を止めたいときは、［なし］を選択します。

7. ［設定］ボタンをクリックします。

これで、Webブラウザで見たいホームページのURLを指定したり、メールソフトで送受信の操作をしたりすると、自動的に回線をつないで相手先（プロバイダ）に接続できます。また、回線の接続中は、LANポートにつないだほかのパソコンでも、接続操作を行ったパソコンと同様に、インターネット上のサービスを利用できます。

◆［自動接続相手先2］について

［自動接続相手先2］を利用すると、1の相手先が話中などで接続できないとき、2の相手先に接続したり、時間帯によって接続する相手先を切り替えることができます。詳しくは、**「時間によって自動接続するプロバイダを変更する」〈P.32〉を参照して****ください。**

◆自動接続できなくなる場合

購入時の設定では、相手先には自動接続の制限が設定されています（料金による制限・接続回数による制限・最大接続時間経過後の自動接続・時間帯による制限）。どれかの制限を超えると、その相手先には自動接続されなくなります。自動接続の制限を解除する方法は、**「自動接続制限状況を見る／制限を解除する」〈P.41〉を参照して****ください。**

指定時間内だけ自動接続する

自動接続可能な時間帯を制限できます。時間帯は、相手先ごとに開始時刻と終了時刻を指定して設定します。

◆ 意図していない接続を行うことがあります。
ネットワークやパソコンの設定内容や運用によっては、回線が接続したままになっていたり、意図していない自動接続を行うことがあります。（例えば、一部のWebサイトではサーバから情報を送り続けるものがあります。）お客様の意図していない接続について、弊社は一切責任を負いかねますので、あらかじめご了承ください。
とくに端末型ダイヤルアップ接続の場合は、本製品の導入後しばらくは、接続の状況や通信料金にご注意ください。接続の状況や通信料金は次の場所で確認することができます。

- 本体のランプ　→　回線接続中は、ISDNをご利用の場合はB1またはB2ランプが点灯します。
  ※ブロードバンドの場合は、WANランプやPPPoEランプが点灯します。設定によっては、PPPoEランプは点灯しないことがあります。
- 設定ページの［切断／接続状況］画面→「接続状況を確認する」〈P.86〉
- 設定ページの［情報表示（通信料金）］画面→「通信料金情報を見る／消去する」〈P.92〉

また、次の環境では本製品を使用しないように注意してください。

- すでに稼働しているLANに本製品を導入するとき、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行うことは避けてください。
- LANポートにつないだパソコンで、定期的に回線を接続して通信を行うソフトウェアを起動したままにしないでください。

設定ページ

1. 本製品に時刻を正しく設定します。

※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。

→「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［＃０］～［＃１５］の中から、接続時間を制限したい相手先の番号をクリックします。ここでは、［#8］をクリックします。

クリックした番号の［接続／相手先登録］画面が表示されます。

3. ［以下の情報を登録する］をクリックします。

4. ［発信］の各項目で、次のように設定します。

項目	設定
相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動接続制限］の項目で、次のように設定します。

時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	「12:00」時：分から「19:00」時：分まで 自動接続可能な時間帯の開始時刻と終了時刻を入力します。 ※曜日の指定はできません。
終了時刻で強制切断	する 終了時刻になったら自動切断するときに［する］を選択します。 ※［する］に設定すると、自動切断／手動接続に関わらず、終了時刻になると通信中でも自動切断します。 ※［しない］に設定すると、自動接続可能な時間帯が過ぎても、回線を切断しません。

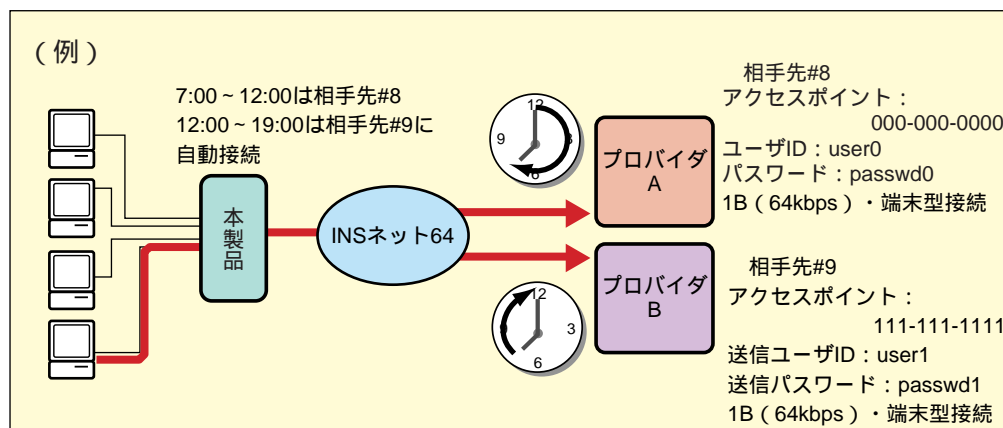
時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	12:00 時:分から 19:00 時:分まで
終了時刻で強制切断	○しない ⊙する

6. ［実行］ボタンをクリックします。

7. 自動接続可能な時間帯を設定した相手先を、「自動接続する」の要領で自動接続相手先に設定します。

   以降、この相手先へは、12:00〜19:00の間のみ自動接続できます。なお、12:00〜19:00以外の時間帯は自動接続できません。手動で接続してください。

時間によって自動接続するプロバイダを変更する

［接続／相手先登録］画面で自動接続可能な時間帯を設定し、［自動接続相手先］画面で自動接続相手先を2つ設定することで、時間帯によって自動接続する相手先を切り替えることができます。

■プロバイダの設定

設定ページ

1. **本製品に時刻を正しく設定します。**

   ※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。
   →「時刻を設定する/修正する」〈P.81〉

2. **［詳細設定］をクリックし、［接続／相手先登録］→［#0］〜［#15］の中から、1つめの相手先（プロバイダ）の番号をクリックします。ここでは、［#8］をクリックします。**

   クリックした番号の［接続／相手先登録］画面が表示されます。

3. ［以下の情報を登録する］をクリックします。

4. ［相手先情報］［発信］の各項目で、1つめの相手先の設定をします。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user0 ※「no」「clear」は使用できません。
送信パスワード	passwd0 ※「no」「clear」「＊（1 文字)」「？（1 文字)」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動接続制限］の項目で、次のように設定します。

時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	「7:00」時：分から「12:00」時：分まで 1つめの相手先に自動接続する時間帯の開始時刻と終了時刻を入力

時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	7:00 時:分から 12:00 時:分まで
終了時刻で強制切断	○しない ⊙する

6. ［実行］ボタンをクリックします。

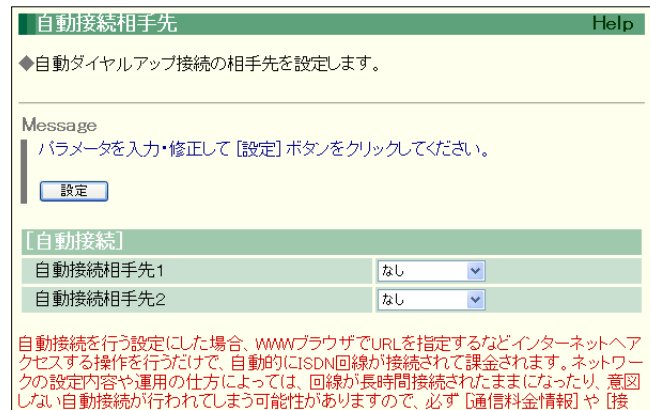
7. ［接続／相手先登録］→［#9］をクリックします。
クリックした番号の［接続／相手先登録］画面が表示されます。

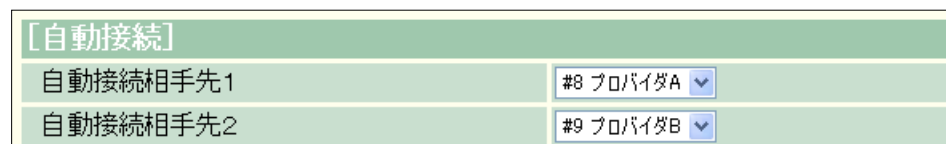
8. ［相手先情報］［発信］の各項目で、2つめの相手先の設定をします。

相手先名称	名称（何でも構いません。例：プロバイダ B）を設定 ※「no」「clear」は使用できません。
相手先電話番号	111-111-1111
送信ユーザ ID	user1 ※「no」「clear」は使用できません。
送信パスワード	passwd1 ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

9. ［自動接続制限］の項目で、次のように設定します。

時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	「12:00」時：分から「19:00」時：分まで 2つめの相手先に自動接続する時間帯の開始時刻と終了時刻を入力

時間帯による制限	以下の時間帯のみ自動接続可能
自動接続可能な時間帯	12:00 時:分から 19:00 時:分まで
終了時刻で強制切断	○しない ⊙する

10. ［実行］ボタンをクリックします。

■自動接続相手先の設定

設定ページ

1. ［詳細設定］をクリックし、［自動接続相手先］をクリックします。

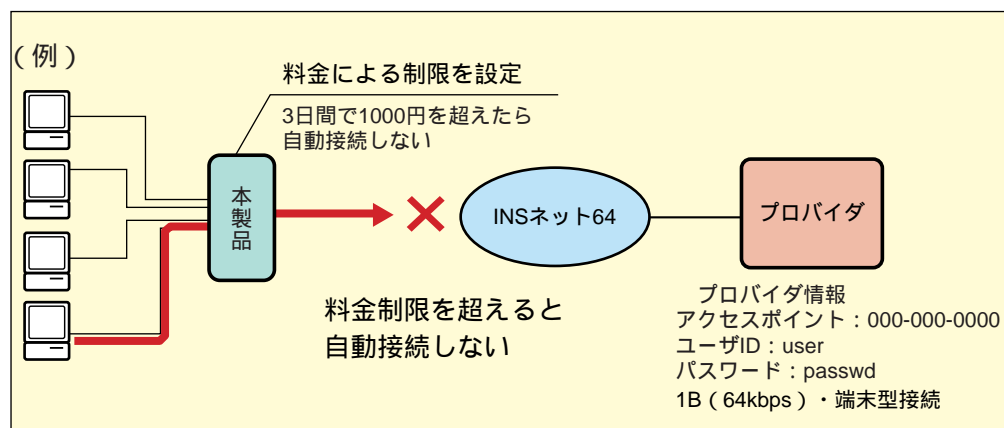
   ［自動接続相手先］画面が表示されます。

2. ［自動接続相手先１］は［#8］を、［自動接続相手先２］は［#9］を選択します。

3. ［設定］ボタンをクリックします。

   これで、7:00〜12:00は相手先＃8に登録したプロバイダに、12:00から19:00は相手先＃9に登録したプロバイダに自動接続されます。
   19:00〜7:00は、どちらのプロバイダにも自動接続されません。

一定通信料金を超えたら自動接続しない

一定の通信料金を超えると自動接続しないように、通信料金の制限を設定できます（この場合、手動での接続は可能です）。通信料金の制限では、相手先ごとに一定期間あたりの自動接続可能な料金を設定します。

◆通信料金は回線切断後に確定します。

通信料金は、回線切断後に［情報表示（自動接続制限）］画面の［料金制限（現在）］に表示されます。回線接続中の通信料金は反映されません。

◆通信料金は、実際の料金請求額と異なることがあります。

◆料金による制限は、あくまでも目安です。
［情報表示（接続／切断ログ）］画面や［情報表示（通信料金）］画面などを確認しながら使ってください。

◆通信料金による自動接続制限が正しく働かない場合

次の場合は、ISDN回線網から料金情報が通知されないため、通信料金による自動接続制限が正しく働きません。
- **電話をかける際に、「0033（NTTコミュニケーションズ）」「001（KDDI株式会社）」「0088（日本テレコム株式会社）」などの番号を付けた場合**
- **PHS電話機に発信した場合**
- **PHS電話機を利用した機器にPIAFSで発信した場合**
- **本製品に接続したFOMA/PHS/モデムの対応PCカードから発信した場合**

なお、ブロードバンドの場合は、接続時間に応じた通信料金は必要でないので、通信料金による自動接続制限の対象外になります。

◆ネットワークの設定や運用によっては正しく動作しないことがあります。

設定ページ

1. **本製品に時刻を正しく設定します。**

   ※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。

   →「時刻を設定する/修正する」〈P.81〉

2. **［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、自動接続を制限したい相手先の番号をクリックします。ここでは、［#8］をクリックします。**

   クリックした番号の［接続／相手先登録］画面が表示されます。

3. **［以下の情報を登録する］をクリックします。**

4. **［相手先情報］［発信］の各項目で、次のように設定します。**

項目	設定
相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動接続制限］の［料金による制限］で、「1000/3」と入力します。

「通信料金（10〜100,000円）／期間（1〜7日）」の形式で入力します。

［自動接続制限］	
料金による制限	1000/3 円／日

※「0」を入力すると、通信料金を制限しないことになります。

6. ［実行］ボタンをクリックします。

7. 通信料金による制限を設定した相手先を、「自動接続する」の要領で自動接続相手先に設定します。

図の例では、以降この相手先への接続でかかった通信料金が3日過ぎるより先に1,000円を超えた場合、この相手先には自動接続されません。

◆料金制限を解除する方法

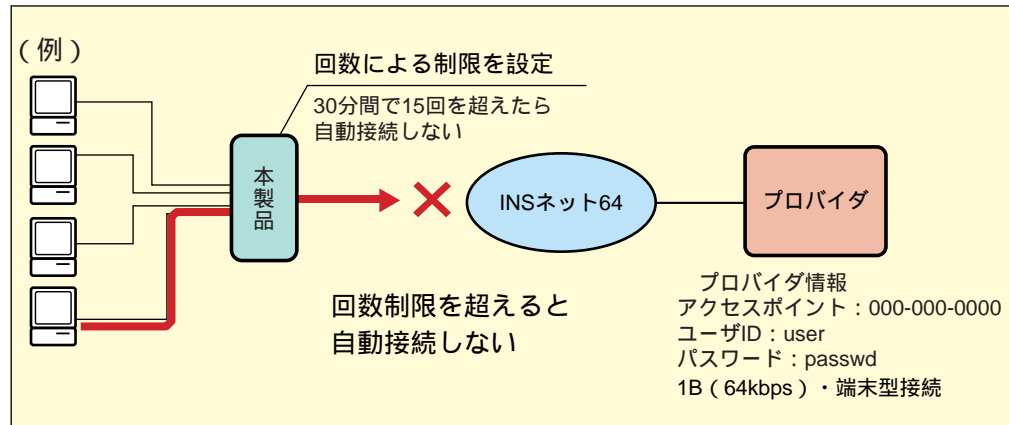
積算された通信料金が制限を超えて、自動接続しなくなったときに再び自動接続したい場合は、次のいずれかの操作を行ってください。

- **［接続／相手先登録］画面の［料金による制限］の金額を増やして再度設定する。**
- **［情報表示（自動接続制限）］画面で料金制限をリセットする→****「自動接続状況を見る/制限を解除する」〈P.41〉**

◆通信中に通信料金が制限を超えた場合

自動接続できなくなるのは、設定した通信料金を超えたときに行っていた通信を終えてからです。長時間接続していると、設定した金額を大幅に超えてしまうことがあるのでご注意ください。

一定回数を超えたら自動接続しない

自動接続できる回数の制限を設定できます（回数の制限を超えた場合でも、手動では接続できます）。回数の制限は相手先ごとに、一定時間あたりの自動接続可能な回数を設定します。

◆接続回数による制限は、あくまでも目安です。
［情報表示（接続／切断ログ）］画面や［情報表示（通信料金）］画面などを確認しながら使ってください。

◆ネットワークの設定や運用によっては正しく動作しないことがあります。

設定ページ

1. 本製品に時刻を正しく設定します。

※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。
→「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［＃0］～［＃15］の中から、自動接続を制限したい相手先の番号をクリックします。ここでは、［＃8］をクリックします。

クリックした番号の［接続／相手先登録］画面が表示されます。

接続／相手先登録#8　Help

◆相手先の情報を登録したり、相手先に回線を手動で接続します。

Message
パラメータを入力・修正し、操作を選んで［実行］ボタンをクリックしてください。

送信パスワード／受信パスワード／鍵配送鍵は、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

◉ 以下の情報を登録する。
○ 以下の相手先に回線を接続する。

［実行］［やり直し］

［相手先情報］

相手先名称	
相手先電話番号	

2. ［以下の情報を登録する］をクリックします。

3. ［相手先情報］［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

4. ［自動接続制限］の［接続回数による制限］で、「15/30」と入力します。
「回数（1～9999回）／時間（1～1440分）」の形式で入力します。

接続回数による制限	15/30 回／分

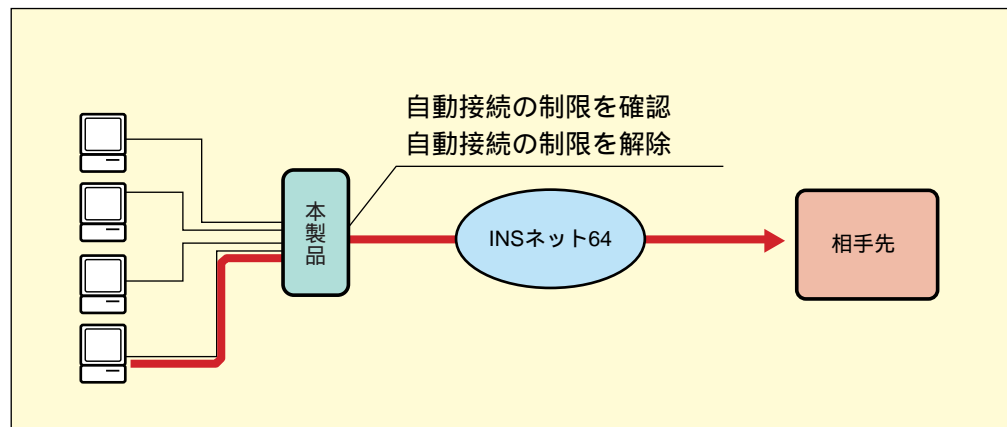
※「0」を入力すると、接続回数を制限しないことになります。

5. ［設定］ボタンをクリックします。

6. 接続回数による制限を設定した相手先を、「自動接続する」〈P.26〉の要領で自動接続相手先に設定します。
図の例では、以降この相手先への30分の間に15回接続した場合、この相手先には自動接続されません。

◆回数制限を解除する方法
「自動接続状況を見る/制限を解除する」〈P.41〉を参照してください。

自動接続制限状況を見る／制限を解除する

設定ページの［情報表示（自動接続制限）］画面では、設定している接続の制限と現在の通信状況を、相手先ごとに確認できます。また、制限によって自動接続できなくなった相手先の制限を解除し、再び自動接続できるようにします。

設定ページ

1. ［詳細設定（またはクイック設定）］をクリックし、［情報表示］→［自動接続制限］をクリックします。

   ［情報表示（自動接続制限）］画面が表示されます。

相手先	料金制限（現在/設定）	回数制限（現在/設定）	再接続制限
#0 プロバイダ（メイン）	制限なし（円） 1/ 7（日）	制限なし（回） 12/ 60（分）	設定中
#1	0/ 3000（円） 1/ 7（日）	0/ 20（回） 12/ 60（分）	設定中
#2 フレッツ・スクウェア(NTT東日本)	制限なし（円） 1/ 7（日）	制限なし（回） 12/ 60（分）	設定中

画面には次のような内容が表示されます。

料金制限（上段）	左側には、この相手に接続したときの通信料金の累計が表示されます（期間が過ぎると0に戻ります）。右側には、設定されている制限料金が表示されます。
料金制限（下段）	左側には、経過期間が表示されます。右側には、料金制限に設定されている期間が表示されます。
回数制限（上段）	左側には、この相手に接続した回数が表示されます（期間が過ぎると0に戻ります）。右側には、設定されている制限回数が表示されます。
回数制限（下段）	左側には、経過期間が表示されます。右側には、回数制限に設定されている期間が表示されます。
再接続制限	最大接続時間（分）通信した後の自動接続が、制限されているかどうかが表示されます。 なし：自動接続は制限されていません。 設定中：自動接続制限が設定されていて、まだ制限されていません。 禁止中：自動接続が制限されています。

2. 制限を解除するときは、［リセットする相手先］で、再び自動接続したい相手先を選択します。

3. 解除したい情報によって、次のいずれかの項目を選択します。

・超過した項目だけをリセットする
積算された情報が、制限を超えた項目だけリセットされます。

・すべての項目をリセットする
積算された情報に関わらず、すべての項目がリセットされます。

4. ［リセット］ボタンをクリックします。
積算された情報がリセットされ、再び0から積算し始めます。

◆通信料金による自動接続制限が正しく働かない場合

次の場合は、ISDN回線網から料金情報が通知されないため、通信料金による自動接続制限が正しく働きません。

- **電話をかける際に、「0033（NTTコミュニケーションズ）」「001（KDDI株式会社）」「0088（日本テレコム株式会社）」などの番号を付けた場合**
- **PHS電話機に発信した場合**
- **PHS電話機を利用した機器にPIAFSで発信した場合**
- **本製品に接続したFOMA/PHS/モデムの対応PCカードから発信した場合**

なお、ブロードバンドの場合は、接続時間に応じた通信料金が必要ではないので、通信料金による自動接続制限の対象とはなりません。

4 切断する

ここでは、回線を切断する方法について解説しています。手動で切断することも、条件を設定して自動で切断することも可能です。

手動で切断する

手動で回線を切断する方法を解説します。切断する前には、他の人がその回線を使って通信しているかどうかを確認してください。

設定ページ

1. ［詳細設定（またはクイック設定）］をクリックし、［切断／接続状況］をクリックします。

2. 切断したい回線やプロトコルなどをクリックします。
   次の画面が表示されます。

※［ISDN］を選択したときの画面です。

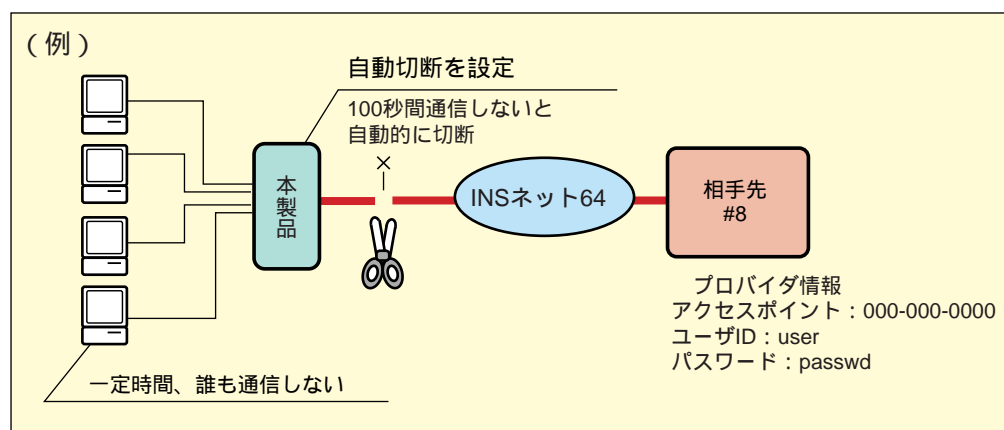
3. 画面下の［接続状況］で現在の接続状況をみて、どのチャネルを切断するかを確認します。

4. ［切断するチャネル］から、切断するチャネル（回線）を選択します。

5. ［切断］ボタンをクリックします。
「○○チャネルを切断しました。」というメッセージが表示され、回線が切断されます。

◆最大接続時間が経過して回線が切断されたとき
最大接続時間経過後の自動接続を禁止している場合、再び自動接続するには［情報表示（自動接続制限）］画面で自動接続制限条件をリセットしてください。→「自動接続制限状況を見る／制限を解除する」〈P.41〉
なお、手動での接続は可能です。

一定時間通信しないとき自動切断する

本製品には、自動切断タイマが搭載されています。インターネットにアクセスし、一定時間回線上で通信がないときは、自動的に回線が接続されます。

◆ 端末型ダイヤルアップ接続の場合、こちらから発信した回線が接続されている間は、課金されます。通信終了後、すぐに回線を切断したいときは手動で回線を切断してください。

◆ 自動切断されないことがあります。

ネットワークやパソコンの設定内容や運用によっては、自動切断されず回線が接続したままになることがあります。（例えば、サーバから情報を送り続けるような一部Webサイトをご利用の場合は、自動切断を設定していても有効にならない場合があります。）お客様の意向どおりに自動切断されなくても、弊社は一切責任を負いかねますので、あらかじめご了承ください。

とくに端末型ダイヤルアップ接続をご利用の場合は、本製品の導入後しばらくは、接続の状況や通信料金にご注意ください。接続の状況や通信料金は次の場所で確認することができます。

- 本体のランプ　→　回線接続中は、ISDNをご利用の場合はB1またはB2ランプが点灯します。
  ※ブロードバンドの場合は、WANランプやPPPoEランプが点灯します。設定によってはPPPoEランプが点灯しないことがあります。
- 設定ページの［切断／接続状況］画面→「接続状況を確認する」〈P.86〉
- 設定ページの［情報表示（通信料金）］画面→「通信料金情報を見る／消去する」〈P.92〉

また、次の環境では本製品を使用しないように注意してください。

- すでに稼働しているLANに本製品を導入するとき、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行うことは避けてください。
- LANポートにつないだパソコンで、定期的に回線を接続して通信を行うソフトウェアを起動したままにしないでください。

次の場合も注意が必要です。
・ 他社製ルータがブロードキャストを送信する場合
・ 本製品に着信がある（本製品をリモートアクセスサーバにしているときなど）場合は、回線を接続した側で回線を切断することをお勧めします。

◆ 自動切断できないときは、手動で切断してください。または、最大接続時間を設定し、長時間接続しないようにしてください。

設定ページ

1. 本製品に時刻を正しく設定します。

※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。

→「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［#0］～［#15］の中から、自動切断したい相手先の番号をクリックします。ここでは、［#8］をクリックします。

クリックした番号の［接続／相手先登録］画面が表示されます。

3. ［以下の情報を登録する］をクリックします。

4. ［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動切断］の［自動切断タイマ1］に、「100」と入力します。［使用するタイマ］で［常にタイマ1］を選択します。

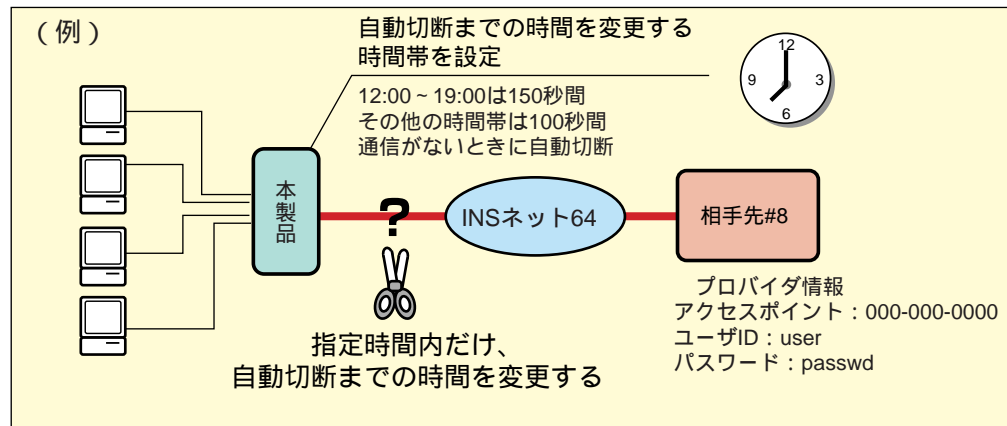
自動切断タイマ1	100 秒
使用するタイマ	常にタイマ1

10〜9999秒の範囲で設定します。
※「0」を入力すると、自動切断されません。

6. ［実行］ボタンをクリックします。

以降、回線を接続後、設定した時間内に通信がないときは、自動的に回線が切断されます。

指定時間内だけ自動切断するまでの時間を変更する

指定した時間内だけ自動切断タイマを変更できます。例えば、会社の就業時間内と就業時間外とで、異なる自動切断タイマを設定したい場合などに使います。時間帯は、相手先ごとに開始時刻と終了時刻を指定して設定します。なお、終了時刻前に回線を切断したいときは、手動で切断してください。

設定ページ

1. 本製品に時刻を正しく設定します。

   ※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。
   →「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［＃0］～［＃15］の中から、指定時間内だけ自動切断の時間を変更したい相手先の番号をクリックします。ここでは、［＃8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

接続／相手先登録#8　Help

◆相手先の情報を登録したり、相手先に回線を手動で接続します。

Message

パラメータを入力･修正し、操作を選んで［実行］ボタンをクリックしてください。

送信パスワード／受信パスワード／鍵配送鍵は、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

◉ 以下の情報を登録する。
○ 以下の相手先に回線を接続する。

［実行］［やり直し］

［相手先情報］

相手先名称

相手先電話番号

［発信］

3. ［以下の情報を登録する］をクリックします。

4. ［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字)」「？（1 文字)」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動切断］の項目で、次のように設定します。

自動切断タイマ1	100 指定する時間帯以外での自動切断までの時間を入力 ※10～9999秒の範囲で入力します。 ※「0」を入力すると、指定時間以外の時間帯では、自動切断しないことになります。
使用するタイマ	タイマ 1、以下の時間帯のみタイマ　2 に変更
自動切断タイマ2	150 指定する時間帯の、自動切断までの時間を入力 ※10～9999秒の範囲で入力します。 ※「0」を入力すると、指定する時間帯では、自動切断しないことになります。
タイマ 2 の時間帯	「12:00」時：分から「19:00」時：分まで 自動切断タイマの値を変更する時間帯の、開始時刻と終了時刻を入力 ※曜日によって、時間帯を変えることはできません。 ※この例では、12時00分に自動切断タイマ2に切り替わり、その時点で150秒以上通信がないと、自動切断します。また、19時00分に自動切断タイマ1に切り替わり、その時点で100秒以上通信がないと自動切断します。

終了時刻で強制切断	する 終了時刻になったら自動切断するときに「する」を選択 ※「する」の場合、終了時刻になると通信中でも自動切断します。なお、自動切断後の自動接続は制限されません。 ※「しない」の場合は、終了時刻になっても回線は切断されません。

自動切断タイマ1	100 秒
使用するタイマ	タイマ1、以下の時間帯のみタイマ2に変更
自動切断タイマ2	150 秒
タイマ2の時間帯	12:00 時:分から 19:00 時:分まで
終了時刻で強制切断	○しない ⊙する

6.［実行］ボタンをクリックします。

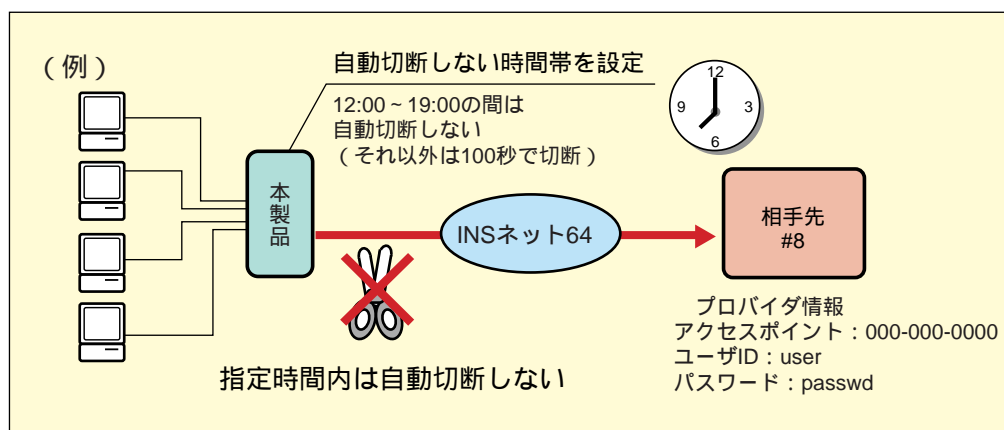
以降、12:00〜19:00は150秒間、それ以外の時間帯では100秒間通信がない場合には、自動的に回線が切断されます。

◆［自動切断タイマ1／2］の設定と自動切断の動作について

［接続／相手先登録］画面の［使用するタイマ］を［タイマ1、以下の時間帯のみタイマ2に変更］に設定しているときは、［自動切断タイマ1］と［自動切断タイマ2］の設定によって、自動切断の動作が次のように異なります。

自動切断タイマの時間		自動切断タイマによる自動切断	最大接続時間による自動切断
自動切断タイマ1	自動切断タイマ2		
10〜9999	10〜9999	自動切断タイマは、時間帯によって切り替わる	常に有効
0	10〜9999	［タイマ 2 の時間帯］以外の時間帯は自動切断しない	常に有効
10〜9999	0	［タイマ 2 の時間帯］は自動切断しない	［タイマ 2 の時間帯］は自動切断しない
0	0	常に自動切断しない	［タイマ 2 の時間帯］は自動切断しない

指定時間内だけ自動切断しない

自動切断を行わない時間帯を設定できます。時間帯は、相手先ごとに開始時刻と終了時刻を指定して設定します。設定した時間帯に自動接続や手動接続すると、終了時刻まで自動切断しません。また、開始時刻よりも前に接続したときも、接続している間に開始時刻を過ぎると、終了時刻まで自動切断しません。終了時刻前に回線を切断したいときは、手動で切断してください。

設定ページ

1. 本製品に時刻を正しく設定します。

   ※時刻は必ず設定してください。正しい時刻が設定されていないと、正しく動作しません。

   →「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［＃0］〜［＃15］の中から、指定時間内だけ自動切断をしない相手先の番号をクリックします。ここでは、［＃8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

3. ［以下の情報を登録する］をクリックします。

4. ［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動切断］の項目で、次のように設定します。

自動切断タイマ1	100 指定する時間帯以外での自動切断までの時間を入力 ※10〜9999秒の範囲で入力します。 ※「0」を入力すると、指定時間以外の時間帯では、自動切断しないことになります。
使用するタイマ	タイマ 1、以下の時間帯のみタイマ　2 に変更
自動切断タイマ2	0 ※「0」を入力すると、指定する時間帯では、自動切断しないことになります。
タイマ 2 の時間帯	「12:00」時：分から「19:00」時：分まで 自動切断タイマの値を変更する時間帯の、開始時刻と終了時刻を入力 ※曜日によって、時間帯を変えることはできません。 ※この例では、12時00分に自動切断タイマ2に切り替わり、19時00までは自動切断しません。また、19時00分に自動切断タイマ1に切り替わり、その時点で100秒以上通信がないと自動切断します。
終了時刻で強制切断	する 終了時刻になったら自動切断するときに「する」を選択 ※「する」の場合、終了時刻になると通信中でも自動切断します。なお、自動切断後の自動接続は制限されません。 ※「しない」の場合は、終了時刻になっても回線は切断されません。

自動切断タイマ1	100 秒
使用するタイマ	タイマ1、以下の時間帯のみタイマ2に変更
自動切断タイマ2	0 秒
タイマ2の時間帯	12:00 時:分から 19:00 時:分まで
終了時刻で強制切断	○しない ⊙する

6.［実行］ボタンをクリックします。

以降、12:00〜19:00間は、自動切断されません。

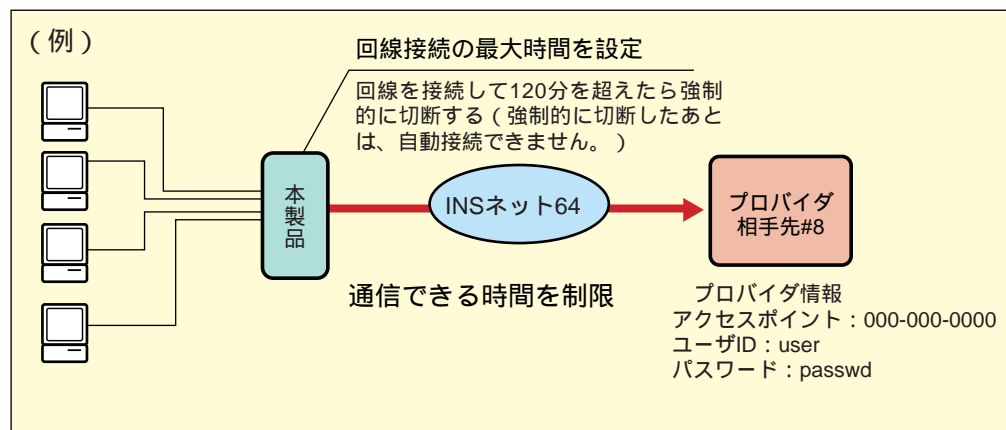
◆端末型ダイヤルアップ接続で通信料金を制限している場合

本製品で通信料金を制限している場合は、INSネットから通知される料金情報によって通信料金を積算します。INSネット64のテレホーダイを利用する場合も、通常の通信時と同様にINSネットから接続時間あたりの料金情報が通知されます。そのため、テレホーダイの時間帯には自動切断をしないように設定していると、本製品で積算した通信料金と、実際の通信料金の差が大きくなることがあります。そのため、実際の通信料金が制限を超える前に、自動接続できなくなることがあります。通信料金の制限について詳しくは、「一定通信料金を越えたら自動接続しない」〈P.36〉を参照してください。

5 通信時間

回線を接続してから切断するまでの、通信時間について設定することができます。

1回の接続で通信できる時間を制限する

回線を接続していられる最大時間を相手先ごとに設定できます。

回線接続後、設定した時間が経過すると、通信中でも回線が切断されます。

設定ページ

1. 本製品に時刻を正しく設定します。

→「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［接続／相手先登録］→［＃0］～［＃15］の中から、通信時間を制限したい相手先の番号をクリックします。ここでは、［＃8］をクリックします。

   クリックした番号の［接続／相手先登録］画面が表示されます。

3. ［以下の情報を登録する］をクリックします。

4. ［発信］の各項目で、次のように設定します。

相手先名称	名称（何でも構いません。例：プロバイダ A）を設定 ※「no」「clear」は使用できません。
相手先電話番号	000-000-0000
送信ユーザ ID	user ※「no」「clear」は使用できません。
送信パスワード	passwd ※「no」「clear」「＊（1 文字）」「？（1 文字）」は使用できません。
通信チャネル	1B（64kbps）
接続モード	端末型接続

5. ［自動切断］の［最大接続時間］と、［自動接続制限］の［最大接続時間経過後の自動接続］で、次のように設定します。

最大接続時間	120 分単位で、10～9999分の範囲で入力 ※接続時間を制限しないときは、「0」を入力します。
最大接続時間経過後の自動接続	不許可 ※設定した時間が経過して回線を切断したあと、自動接続したくないときは、［不許可］を選択します。

最大接続時間	120 分
最大接続時間経過後の自動接続	◉不許可 ○許可

6. ［実行］ボタンをクリックします。

以降、この相手先に回線を接続してから120分経過すると、自動的に回線が切断されるようになります。

◆最大接続時間が経過して回線が切断されたとき

最大接続時間経過後の自動接続を禁止している場合、再び自動接続するには［情報表示（自動接続制限）］画面で自動接続制限条件をリセットしてください。→「自動接続制限状況を見る／制限を解除する」〈P.41〉

なお、手動での接続は可能です。

6 メール着信通知

ここでは、電子メールの着信を確認する方法や、着信した電子メールを読んだり削除したりする方法を解説します。

メール着信通知機能について

パソコンを起動しなくても、プロバイダのメールサーバに電子メールが到着しているかどうか、本製品が自動的に確認して通知します。電子メールが着信すると、本体前面のランプ（MAIL）が緑色に点滅します。また、本製品の設定ページでもメールの着信を確認できます。

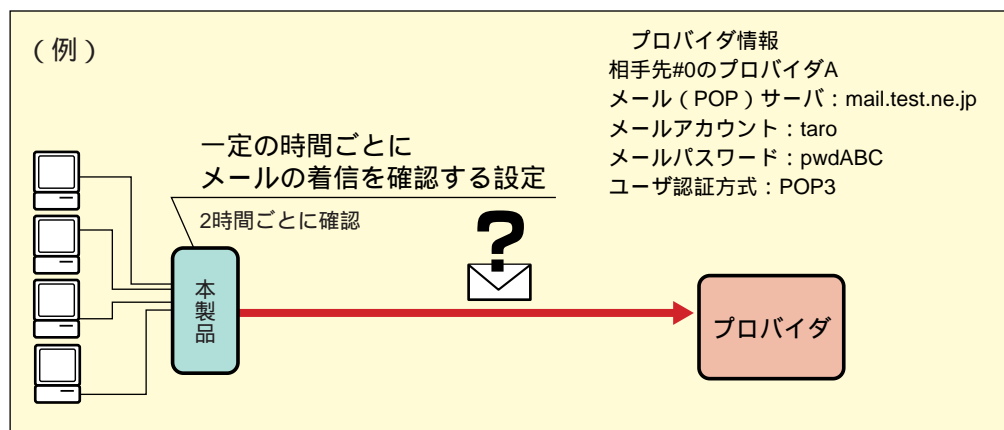
◆次の点にご注意ください

- 端末型ダイヤルアップ接続の場合、メールの着信を確認するために回線を接続するたび、接続時間に応じた通信料金がかかります。
- 自動接続を制限しているときは、メールの確認は自動的には行われません。
- 自動接続の制限によって自動接続できないときで、電子メールの有無を確認できるのは次の場合です。
  - ・すでに回線が接続されていて、確認する時刻になったとき
  - ・設定ページで手動でメール確認を行ったとき

◆確認の対象となる電子メールについて

本製品では、最新の電子メールから200件目までが確認の対象になります。メールサーバに200件以上残っている場合、201件以前の電子メールは確認しないので、通知すべき未読メールがあっても通知されません。

指定した時間間隔でメールの着信を確認する

「30分ごと」や「2時間ごと」など、一定の時間ごとに電子メールの着信を確認する設定方法を解説します。

端末型ダイヤルアップ接続の場合、この操作を行うと本製品が定期的にインターネットに接続してメールの有無を確認します。インターネットに接続するたびに、接続時間に応じた通信料金がかかります。

設定ページ

1. **本製品に時刻を正しく設定します。**

   →「時刻を設定する/修正する」〈P.81〉

2. **［詳細設定］をクリックし、［メール設定／一覧］→［メール着信通知設定］をクリックします。**

   ［メール設定/一覧（メール着信通知設定）］画面が表示されます。

メール設定／一覧（メール着信通知設定）　Help

◆メール着信通知に関するパラメータを設定します。

Message

パラメータを入力・修正して［設定］ボタンをクリックしてください。

メールパスワードは、どのような文字列を設定しても「＊」または「●」の1文字が表示されます。
変更するときは、表示されている「＊」または「●」を消去してから、新しい文字列を入力してください。

［設定］［やり直し］

［メール着信通知］	
メール着信自動通知	◉しない ○する
確認時間	時刻（時:分/日間隔）で設定
時刻（時:分/日間隔） 時間間隔（分）	
接続する相手先	#0 プロバイダ（メイン）
［メール受信］	
メール（POP）サーバ	
メールアカウント	

3. ［メール着信通知］［メール受信］の項目で、次のように設定します。

メール着信自動通知	する
確認時間	時間間隔（分）で設定
時刻（時:分/日間隔） 時間間隔（分）	120 ※10〜1440分の範囲で、確認の間隔を10分単位で入力します。 ※自動接続できる時間帯を設定しているときは、その時間内だけメール着信の確認を行います。そのほか、自動接続を制限しているときは、メール着信確認の接続も制限の対象になります。
接続する相手先	#0 プロバイダA ※#0〜#15を選択すると［接続/相手先登録］画面で設定している相手先に接続します。あらかじめ、相手先を登録してください。 ※Ethernetは、メールサーバがこちら側のLAN上にあるときに選択します。 または、［自動接続相手先］で登録されている相手先、PPPoE を採用していないプロバイダのいずれかのメールサーバにアクセスするときに選択します。
メール（POP）サーバ	mail.test.ne.jp
メールアカウント	taro ※プロバイダに接続するためのアカウントとは別のものです。「メールアカウント」はプロバイダから通知されたものを入力してください。 ※大文字と小文字は別の文字として扱われます。 ※「no」「clear」は使用できません。
メールパスワード	pwdABC ※大文字と小文字は別の文字として扱われます。 ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
ユーザ認証	標準（POP3） ※プロバイダから指定された認証方法を選択してください。

［メール着信通知］

メール着信自動通知	○しない ◉する
確認時間	時間間隔(分)で設定
時刻(時:分/日間隔) 時間間隔(分)	120
接続する相手先	#0 プロバイダA
［メール受信］	
メール(POP)サーバ	mail.test.ne.jp
メールアカウント	taro
メールパスワード	••••••
ユーザ認証	標準(POP3)

※［メール（POP）サーバ］〜［ユーザ認証］までの設定は、プロバイダから通知された内容を設定します。

4. ［設定］ボタンをクリックします。

以降、電子メールの有無を本製品が自動的に確認し、本体前面のMAILランプで通知します。

◆接続する相手先で［Ethernet］を選択するときの注意

［Ethernet］を選択すると、LAN上のメールサーバへ着信の確認が行われます。LAN上にメールサーバがない場合は、［自動接続相手先設定］に従って回線の接続を行います。このとき回線の接続ごとに料金が必要な契約をしている場合は、接続料金がかかります、とくに、端末型ダイヤルアップ接続をご利用の場合は注意してください。

◆メール転送について

［メール転送］の項目を設定すると、着信した電子メールを別のメールアドレスに転送できます。→「7.メール転送」〈P.72〉

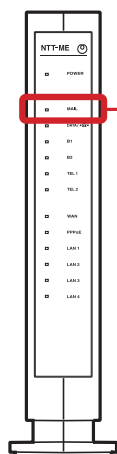
◆通知するメールの種類（フィルタ）について

［通知するメールの種類（フィルタ）］の項目を設定すると、特定の電子メールの着信だけを通知できます。→「特定のメールだけ確認する（フィルタ）」〈P.66〉

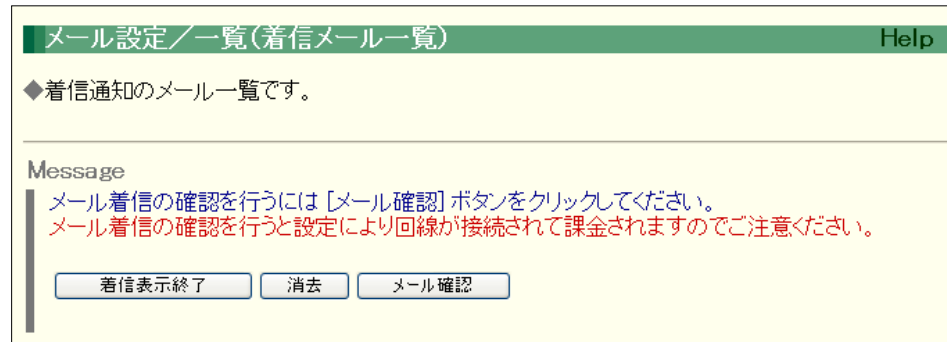
◆自動確認が行われなくなったら

「困ったときは」の「メール着信通知機能で自動確認が行われなくなった」〈P.122〉を参照してください。

■電子メールが着信したら（着信通知状態）

本体前面のランプが点滅し、着信通知状態になります。電子メールの内容はパソコンなどで確認してください。

■ランプの点滅を止めるとき

操作

1. ［詳細設定］をクリックし、［メール設定／一覧］→［着信メール一覧］をクリックします。
   ［着信メール一覧］画面が表示されます。

2. ［着信表示終了］ボタンをクリックします。
   MAILランプの点滅が止まります。

指定した時刻にメールの着信を確認する

「3日ごとの12:00」や「毎日10:00と17:00」など、日にちの間隔と時刻を指定して電子メールの着信を確認する設定方法を解説します。

端末型ダイヤルアップ接続の場合、この操作を行うと本製品が定期的にインターネットに接続してメールの有無を確認します。インターネットに接続するたびに、接続時間に応じた通信料金がかかります。

設定ページ

1. 本製品に時刻を正しく設定します。

→「時刻を設定する/修正する」〈P.81〉

2. ［詳細設定］をクリックし、［メール設定／一覧］→［メール着信通知設定］をクリックします。

［メール着信通知設定］画面が表示されます。

3. ［メール着信通知］［メール受信］の項目で、次のように設定します。

メール着信自動通知	する
確認時間	時刻（時:分/日間隔）で設定
時刻（時:分/日間隔） 時間間隔（分）	9:00,14:00,17:00/1 ※時刻は24時間表記で、「XX:XX」の形式で入力します。 ※時刻を「,」（半角コンマ）で区切って、5つまで入力できます。 ※時刻と日にちの間隔は「/」（半角スラッシュ）で区切ります。日にちの間隔は1～7の範囲で設定してください。 ※自動接続できる時間帯を設定しているときは、その時間内だけメール着信の確認を行います。そのほか、自動接続を制限しているときは、メール着信確認の接続も制限の対象になります。 ※［時刻（時:分/日間隔）］では、次のように入力します。 例1）3日おきに18:00に確認したいとき →18:00/3と入力 例2）毎日10:00、12:00、18:00に確認したいとき → 10:00,12:00,18:00/1と入力
接続する相手先	#0 プロバイダA ※#0～#15を選択すると［接続/相手先登録］画面で設定している相手先に接続します。あらかじめ、相手先を設定してください。 ※Ethernetは、メールサーバがこちら側のLAN上にあるときに選択します。 または、［自動接続相手先］で登録されている相手先、PPPoE を採用していないプロバイダのいずれかのメールサーバにアクセスするときに選択します。
メール（POP）サーバ	mail.test.ne.jp
メールアカウント	taro ※プロバイダに接続するためのアカウントとは別のものです。「メールアカウント」プロバイダから通知されたものを入力してください。 ※大文字と小文字は別の文字として扱われます。 ※「no」「clear」は使用できません。
メールパスワード	pwdABC ※大文字と小文字は別の文字として扱われます。 ※「no」「clear」「＊（1文字）」「？（1文字）」は使用できません。
ユーザ認証	標準（POP3） ※プロバイダから指定された認証方法を選択してください。

[メール着信通知]	
メール着信自動通知	○しない ⊙する
確認時間	時刻(時:分/日間隔)で設定
時刻(時:分/日間隔) 時間間隔(分)	9:00,14:00,17:00/1
接続する相手先	#0 プロバイダA
[メール受信]	
メール(POP)サーバ	mail.test.ne.jp
メールアカウント	taro
メールパスワード	••••••
ユーザ認証	標準(POP3)

※[メール(POP)サーバ]～[ユーザ認証]までの設定は、プロバイダから通知された内容を設定します。

4. [設定]ボタンをクリックします。

以降、電子メールの有無を本製品が自動的に確認し、本体前面のランプで通知します。

◆電子メールが着信したら

電子メールが着信したら、本体前面のMAILランプが点滅します。点滅を止めるときは、設定ページへを使います。「電子メールが着信したら」〈P.60〉～「ランプの点滅を止めるとき」〈P.61〉を参照してください。

◆接続する相手先で[Ethernet]を選択するときの注意

[Ethernet]を選択すると、LAN上のメールサーバへ着信の確認が行われます。LAN上にメールサーバがない場合は、[自動接続相手先設定]に従って回線の接続を行います。このとき回線の接続ごとに料金が必要な契約をしている場合は、接続料金がかかります、とくに、端末型ダイヤルアップ接続をご利用の場合は注意してください。

◆メール転送について

[メール転送]の項目を設定すると、着信したメールを別のメールアドレスに転送できます。→「7.メール転送」〈P.72〉

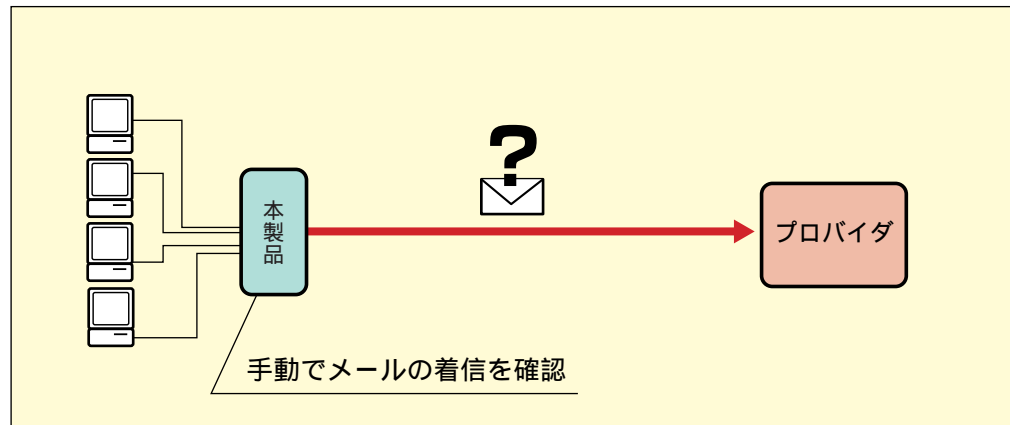
◆通知するメールの種類(フィルタ)について

[通知するメールの種類(フィルタ)]の項目を設定すると、特定の電子メールの着信だけを通知できます。→「特定のメールだけ確認する(フィルタ)」〈P.66〉

◆自動確認が行われなくなったら

「困ったときは」の「メール着信通知機能で自動確認が行われなくなった」〈P.122〉を参照してください。

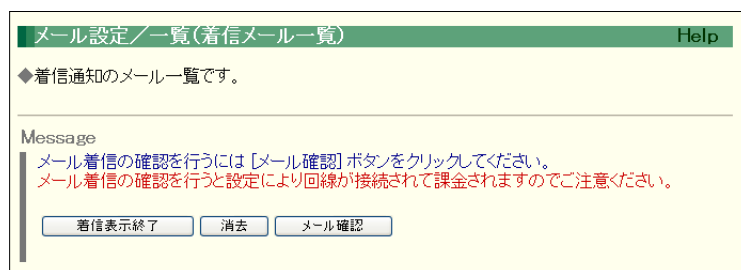
手動ですぐにメールの着信を確認する

［着信メール一覧］画面の［メール確認］ボタンをクリックすると、電子メールの着信の有無をすぐに確認できます。メールが着信している場合は、本体前面のMAILランプが緑色に点滅しています。

端末型ダイヤルアップ接続の場合、この操作を行うと本製品がインターネットに接続してメールの有無を確認します。インターネットに接続するたびに、接続時間に応じた通信料金がかかります。

設定ページ

1. メール着信通知の設定をします。

→「指定した時間間隔でメールの着信を確認する」〈P.58〉または「指定した時刻にメールの着信を確認する」〈P.62〉

2. ［詳細設定］をクリックし、［メール設定／一覧］→［着信メール一覧］をクリックします。

［着信メール一覧］画面が表示されます。

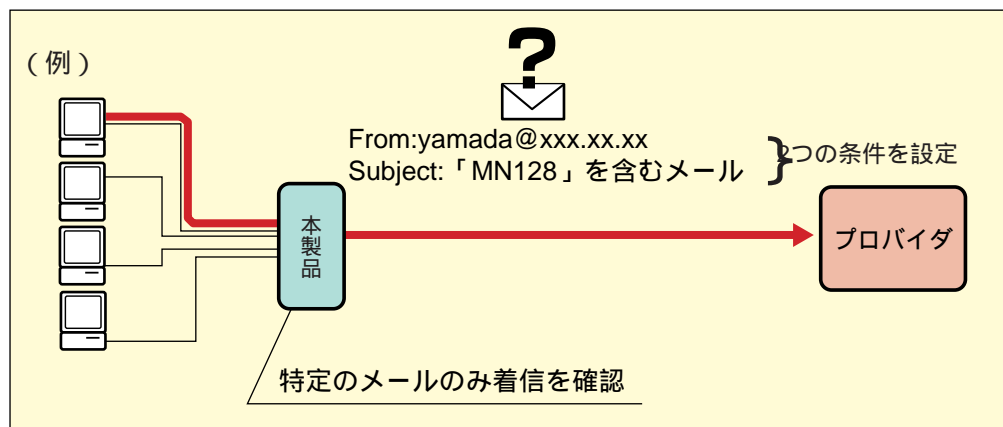
3. ［メール確認］ボタンをクリックします。

本製品がメールサーバにアクセスして、電子メールが届いているかどうか確認します。

4. 電子メールの確認が終了したら、Webブラウザの［更新］ボタンをクリックします。

電子メールが届いているときは、［着信メール一覧］画面にメールが表示されます。
電子メールが届いていないときは、「メールは1件もありません。」と表示されます。

特定のメールだけ確認する（フィルタ）

条件に合う電子メールが届いているときだけ通知するようにできます。

設定ページ

1. ［メール着信通知設定］画面で、メール着信通知の設定をします。

→「指定した時間間隔でメールの着信を確認する」〈P.58〉または「指定した時刻にメールの着信を確認する」〈P.62〉

2. ［通知するメールの種類（フィルタ）］の項目で条件を設定します。

ここでは、送信者が「yamada@xxx.xx.x.x」、またはメールの件名に「MN128」という文字を含んでいるメールだけを確認するときの条件を設定します。

条件	その行の設定内容を有効にするときにチェックします。ここでは、条件を2つ設定するので、1と2をチェックします。
フィールド	条件を適用するメールの項目を選択します。 ［Cc が］→同報するアドレスを条件にしたいときに選択します。 ［From が］→ メール送信元のアドレスを条件にしたいときに選択しします。 ［Subject が］→メールの Subject に含まれる文字を条件にしたいときに選択します。 ［To が］→メール送信先のアドレスをしたいときに選択します。 ここでは、1 行目が［From が］を、2 行目が［Subject が］を選択します。
文字列	条件にする文字列を入力します。半角で128文字、全角で64文字で入力してください。 ここでは、次のように入力します。 1行目 → yamada@xxx.xx.xx 2行目 → MN128

照合	届いたメールと［文字列］の照合方法を選択します。 ［で始まる］→ 入力した文字列で始まるメールを検索します。 ［で終わる］→入力した文字列で終わるメールを検索します。 ［と一致する］→入力した文字列と一致するメールを検索します。 ［を含まない］→入力した文字列を含んでいないメールを検索します。 ［を含む］→入力した文字列を含んでいるメールを検索します。 ［と一致しない］→ 入力した文字列が一致しないメールを検索します。 ここでは、1 行目が［と一致する］を、2 行目が［を含む］を選択します。
フィルタリング	メールの到着を通知するかどうかを選択します。 ［メールを通知する］→届いたメールが設定した条件に合致しているときに、通知します。 ［メールを通知しない］→届いたメールが設定した条件に合致していると、通知しません。 ［メールを通知 + 転送する］→届いたメールが設定した条件に合致しているときに通知し、さらに設定されているアドレスへ転送します。 ここでは、どちらも［メールを通知する］を選択します。
その他のメール	条件 1 ～ 8 の設定条件に該当しないメールの到着を、通知するかどうかを選択 ここでは、［メールは通知しない］を選択します。

[通知するメールの種類(フィルタ)]

条件	フィールド	文字列	照合	フィルタリング
☑1	Fromが	yamada@xxx.xx.xx	と一致する	メールを通知する
☑2	Subjectが	MN128	を含む	メールを通知する
☐3	Subjectが		を含む	メールを通知する
☐4	Subjectが		を含む	メールを通知する
☐5	Subjectが		を含む	メールを通知する
☐6	Subjectが		を含む	メールを通知する
☐7	Subjectが		を含む	メールを通知する
☐8	Subjectが		を含む	メールを通知する
その他のメール				メールは通知しない

3. ［設定］ボタンをクリックします。

以降、条件に一致する電子メールだけが通知されます。

◆条件の適用方法

メールサーバに着信したメールは、[通知するメールの種類（フィルタ）］の設定条件と比較されます。比較は、条件番号の小さな方から順に行われ、最初に該当した設定条件に従って処理されます。なお、［条件］にチェックが付いている設定条件だけが適用されます。

（例）［通知するメールの種類（フィルタ）］を次のように設定している場合

［通知するメールの種類(フィルタ)］

条件	フィールド	文字列	照合	フィルタリング
☑1	Subjectが	重要	を含む	メールを通知する
☑2	Fromが	hanako@mn.co.jp	と一致する	メールを通知する
☐3	Toが	taro	を含む	メールを通知する
☑4	Subjectが	IB3	を含む	メールを通知する
☑5	Subjectが	mn128-soho	で始まる	メールは通知しない
☐6	Fromが	mn.co.jp	を含む	メールは通知しない
☑7	Toが	ichiro	を含む	メールを通知する
☑8	Subjectが	memo	を含まない	メールを通知する
その他のメール				メールは通知しない

・Subjectが「重要（MN128-SOHO）」、Fromが「jiro@mn.co.jp」のメールが届いたとき
　→ **1の設定条件に従って通知されます。**

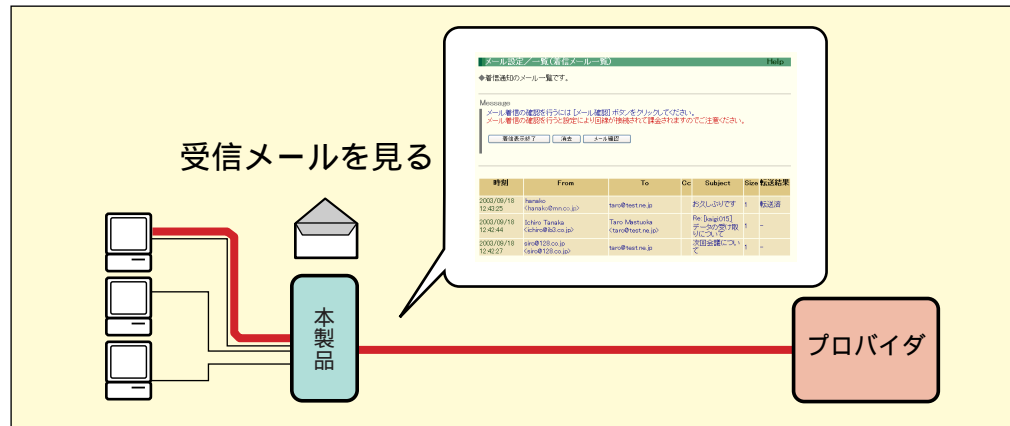
・Toが「ichiro@ib3.co.jp」、Fromが「saburo@mn.co.jp」のメールが届いたとき
　→ **7の設定条件に従って通知されます。（6の設定条件にはチェックが付いていないので適用されません。）**

・Subjectが「memo」、Toが「junko@ib3.co.jp」、Fromが「siro@128.co.jp」のメールが届いたとき
　→ **いずれの設定条件にも該当しないので、［その他のメール］に従って通知されません。**

◆自動確認が行われなくなったら

「困ったときは」の「メール着信通知機能で自動確認が行われなくなった」〈P.122〉を参照してください。

着信したメールを設定ページで見る

設定ページの［着信メール一覧］で、メールの内容を確認できます。

◆電子メールのすべての内容を確認できるわけではありません
この機能では、［メール着信通知設定］画面の［表示する内容］で設定した内容だけが表示されます。また、本文も一部分しか読めないことがあります。確認後は、パソコンからメールソフトなどを使ってメールを受信してください。

◆メールサーバに残っていても、すでに読まれている電子メールは通知しません。

◆一度確認した電子メールは通知しません。

◆確認の対象となる電子メールについて
［メール着信通知設定］画面の［通知するメールの種類（フィルタ）］に適合する電子メールだけを確認できます。**→「特定のメールだけ確認する（フィルタ）」〈P.66〉**

◆電子メールの内容を確認しても、メールサーバから削除されません。

設定ページ

1.［メール着信通知設定］画面で、メール着信通知の設定をします。

→「指定した時間間隔でメールの着信を確認する」〈P.58〉または「指定した時刻にメールの着信を確認する」〈P.62〉

2.［着信メール一覧ページへの表示］で、次のように設定します。

着信メール一覧ページへ表示	する
表示する内容	設定ページに表示したい内容をチェック ※複数の項目を選択可能です。

［着信メール一覧ページへの表示］

着信メール一覧ページへ表示	○しない ⊙する
表示する内容	☑From ☑To ☑Cc ☑Subject ☑Size ☑本文

3.［設定］ボタンをクリックします。

設定ページ

■設定ページからメールを確認する

1. ［詳細設定］をクリックし、［メール設定］→［着信メール一覧］をクリックします。
   ［着信メール一覧］画面が表示されます。

［メール着信通知設定］画面の［表示する内容］で設定した内容だけが表示されます。
各項目の表示は、次のような制限があります。

- To　　：最大で半角128文字まで
- From　：最大で半角32文字まで
- Cc　　：最大で半角128文字まで
- Subject：最大で半角32文字まで
- Size　：制限なし

※最大64件まで表示できます。65件以上になると古い順に消去されます。
※着信メールを消去する方法は「着信したメールを消去する」〈P.71〉を参照してください。
※本体前面のランプの点滅を止めるときは、「ランプの点滅を止めるとき」〈P.71〉を参照してください。

2. 日付をクリックすると、別のウィンドウにそのメールの本文が表示されます。

20行（最大で255文字、半角510文字）まで表示されます。

◆自動確認が行われなくなったら
「困ったときは」の「メール着信通知機能で自動確認が行われなくなった」〈P.122〉を参照してください。

着信したメールを消去する

本製品の電源をOFFにしても、メールは消去されません。消去するときは［着信メール一覧］画面で消去します。

※消去を実行すると、すべてのメールが消去されます。特定のメールだけを消去することはできません。

設定ページ

1. ［詳細設定］をクリックし、［メール設定］→［着信メール一覧］をクリックします。

［着メール一覧］画面が表示されます。

2. ［消去］ボタンをクリックします。

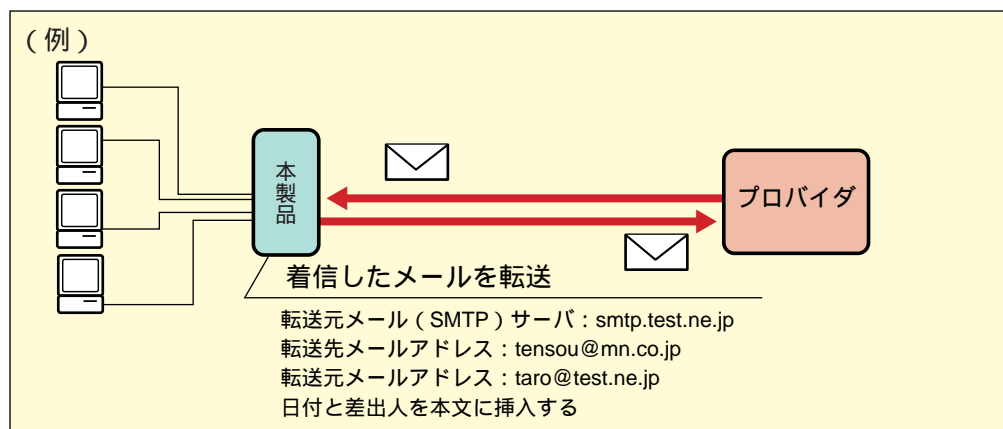
すべてのメールが消去されます。

7 メール転送

メール着信通知機能によって着信を確認したメールを、あらかじめ設定しておいた別のメールアドレスへ転送できます。ここでは、メール転送を行うための設定方法、設定ページに表示される転送結果の見方、メール転送機能のON/OFFの切り替え方を解説します。

◆次の点にご注意ください

- 転送できるのは、メール本文の冒頭20行程度です。
- メールにファイルが添付されている場合、添付ファイルが正しく転送されないことがあります。
- 設定ページの［メール確認］ボタンをクリックしたときは、メール転送は行われません。

着信したメールを転送する

設定ページ

1. メール着信通知の設定をします。
   →「指定した時間間隔でメールの着信を確認する」〈P.58〉または「指定した時刻にメールの着信を確認する」〈P.62〉
2. ［詳細設定］をクリックし、［メール設定］→［着信メール一覧］をクリックします。
   ［着信メール一覧］画面が表示されます。
3. ［メール転送］の項目で、次のように設定します。

メール転送	する
転送元メール (SMTP) サーバ	smtp.test.ne.jp ※プロバイダへから通知されている SMTP サーバの内容に従ってください。 ※省略すると、［メール（POP）サーバ］の内容に従います。
転送先メールアドレス	tensou@mn.co.jp 転送先のメールアドレスを入力 ※ 半角英数字 62 文字以内で入力してください。
転送元メールアドレス	taro@test.ne.jp 転送元のメールアドレスを入力

［メール転送］	
メール転送	○しない ⦿する
転送元メール（SMTP）サーバ	smtp.test.ne.jp
転送先メールアドレス	tensou@mn.co.jp
転送元メールアドレス	taro@test.ne.jp

3. 必要に応じて、［ヘッダを本文へ挿入］と［挿入する内容］を設定します。

ヘッダを本文へ挿入	○しない ⦿する
挿入する内容	☑Date ☑From ☑Subject

電子メールのヘッダ（Subject、From、Date）を本文に含めて転送したいときは、［ヘッダを本文へ挿入］を［する］にします。次に、［挿入する内容］で、本文に挿入するヘッダを選択します。

※転送先が携帯端末で、ヘッダを表示できないときに設定すると便利です。設定すると、転送先には次のように表示されます。

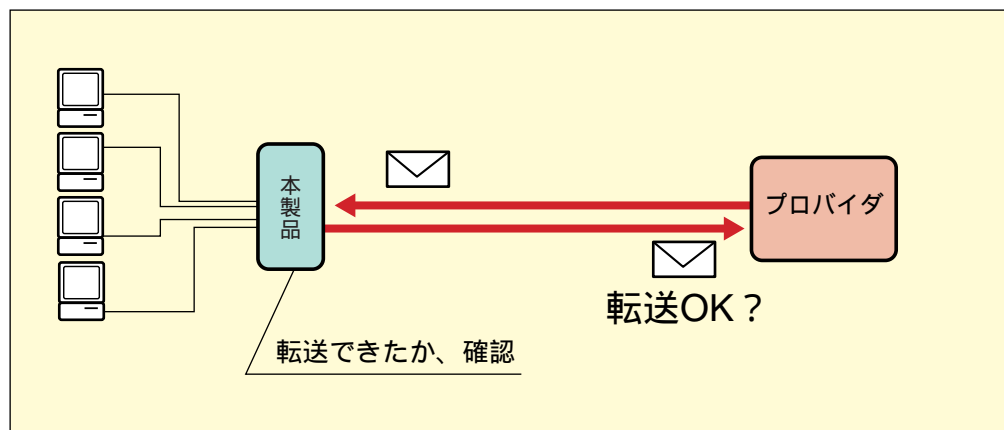
4. ［通知するメールの種類（フィルタ）］で、転送するメールの条件を設定します。

電子メールを転送するときは、［フィルタリング］で［メールを通知+転送する］を選択してください。条件の設定方法については、「特定のメールだけ確認する（フィルタ）」〈P.66〉を参照してください。

5. ［設定］ボタンをクリックします。

以降、電子メールの有無を確認したとき、該当するメールを設定した転送先メールアドレスに転送します。

転送できたかどうか確認する

メールを転送できたかどうかを、［着信メール一覧］画面の［転送結果］欄で確認することができます

転送時にエラーがおきても、メールは再送されません。

設定ページ

1. **［詳細設定］をクリックし、［メール設定／一覧］→［着信メール一覧］をクリックします。**

   ［着信メール一覧］画面が表示されます。

時刻	From	To	Cc	Subject	Size	転送結果
2003/09/18 12:43:25	hanako <hanako@mn.co.jp>	taro@test.ne.jp		お久しぶりです	1	転送済
2003/09/18 12:42:44	Ichiro Tanaka <ichiro@ib3.co.jp>	Taro Mastuoka <taro@test.ne.jp>		Re: [kaigi:015] データの受け取りについて	1	-
2003/09/18 12:42:27	siro@128.co.jp <siro@128.co.jp>	taro@test.ne.jp		次回会議について	1	-

2. **［転送結果］欄を確認します。**

   ［転送結果］欄には、次のように表示されます

   ー　　　：転送しないように設定されているメールです。

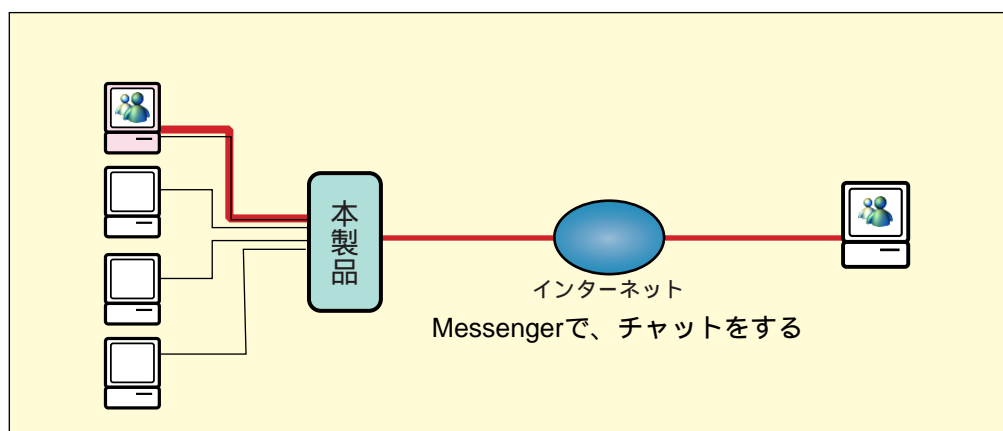
   転送済　：このメールは、設定内容に従って転送されました。

   ※この他のエラーが表示されるときは、**「［メール設定（着信メール一覧）］画面のエラー」〈P.127〉を参照してください。**

8 Messengerを使う

ここでは、音声・ビデオチャットの代表的なソフトウェアの、Windows Messenger、MSN Messengerを本製品で使うときに必要な設定を解説します。

Windows Messenger、MSN Messengerを使う

LANポートにつないだパソコンと、本製品のUPnP（Universal Plug and Play：ユニバーサルプラグアンドプレイ）機能を利用すると、Windows Messenger4.7以上、またはMSN Messenger5.0以上を複数台のパソコンで利用できます。本製品は購入時にUPnP機能がONになっているので、とくに設定をする必要がありません。

◆ Messengerを同時に利用できるパソコンは、4台までです。

◆ UPnPを利用できるパソコンは、Windows XPおよびWindows Meです。
Windows Meの場合は、［コントロールパネル］→［アプリケーションの追加と削除］で［ユニバーサルプラグアンドプレイ］をインストールしてください。

◆ Windows XPをご利用の場合は、［Windows Update］から［Service Pack1］と［重要な更新］のすべてをインストールしてください。

◆ Windows Meをご利用の場合は、DirectX8.1以降をインストールしてください。また、［Windows Update］から［Service Pack1］と［重要な更新］のすべてをインストールしてください。

◆ 電話をかける機能を利用する際には、対応プロバイダとの契約が別途必要です。

◆ 音声チャットを行うには、マイク・スピーカー、またはヘッドセットが別途必要です。

◆ ビデオチャットを行うには、マイク・スピーカー（またはヘッドセット）、カメラ（USBカメラ）などが別途必要です。

■利用できる機能

本製品で利用できるWindows Messenger、またはMSN Messengerの機能は次のとおりです。

OS	Windows XP		Windows Me	
Messenger のバージョン	Windows Messenger 4.7, 5.0	MSN Messenger 5.0, 6.0	MSN Messenger 5.0	MSN Messenger 6.0
インスタントメッセージ	○	○	○	○
音声チャット	○	○	×※2	○※3
ビデオチャット	○	○	－	○※3
電話をかける	－※1	○	○	○
ファイル転送	×※2	○※3	○※3	○※3
アプリケーション共有	○	○	－	－
ホワイトボード	○	○	－	－
リモートアシスタンス	○	○	－	－
同一LAN内同士の音声チャット	○	○	○※3	○※3
同一LAN内同士のファイル送信	○	○	○※3	○※3
同一LAN内同士のビデオチャット	○	○	－	○※3
同一LAN内同士のアプリケーション共有	○	○	－	－
同一LAN内同士のホワイトボード	○	○	－	－

※1　Windows Messenger 4.7、5.0には、電話をかける機能は搭載されていません。
※2　バージョンアップで対応予定です。
※3　UPnP準拠の機能ではありませんが、本製品独自の機能によって利用できます。

Windows Messenger / MSN Messengerがうまく動作しないときは、「困ったときは」の「Windows Messenger / MSN Messengerで通信できない」〈P.121〉をお読みください。

設定ページ

■UPnPポートの自動削除の時間を設定する

MessengerなどUPnP対応の機能を使用することにより、一定時間通信がないとき動的に開いた本製品のポートを自動的に削除することができます。セキュリティ対策のため、自動削除までの時間を設定しておくことをお勧めします。機能によっては通信が開始したときしか使用しないポートがあるため、通信開始から設定時間が経過した際にポートが削除されることがあります。その場合は、次回の通信ができなくなるので、Messengerなどを一度終了し、再度起動してください。

※自動削除までの時間を設定しないときは、Messengerなどからの削除要求か、Messengerで登録した有効期間が過ぎるまでは、ポートは開いたままになります。

1. ［詳細設定］→［UPnP設定］をクリックします。

［UPnP設定］画面が表示されます。

2. ［自動削除まで］の項目で、開いたポートを削除するまでの時間を設定します。

1時間〜24時間まで1時間毎に設定できます。なお、［削除しない］を選択すると、自動削除は行われません。

※24時間以上断続的にMessengerを利用するときは、［削除しない］を選択してください。この場合、ポートを削除するときは、本製品を再起動してください。

3. ［設定］ボタンをクリックします。

以降、登録したポートを使用するMessengerを利用しなくなってから設定した時間が経過すると、ポートが削除されます。

タイマーの設定でポートが削除されたあと、そのポートを使用するMessengerを再度ご利用になる場合は、パソコン側でMessengerをいったん終了してから、再起動してください。

◆UPnPの状況を確認する

［詳細設定（またはクイック設定)］→［情報表示］→［UPnP状況］をクリックすると、Messengerが本製品に対して要求したポートマッピングの状況を確認できます。電源を入れ直すと、ポートマッピングの情報は削除されます。

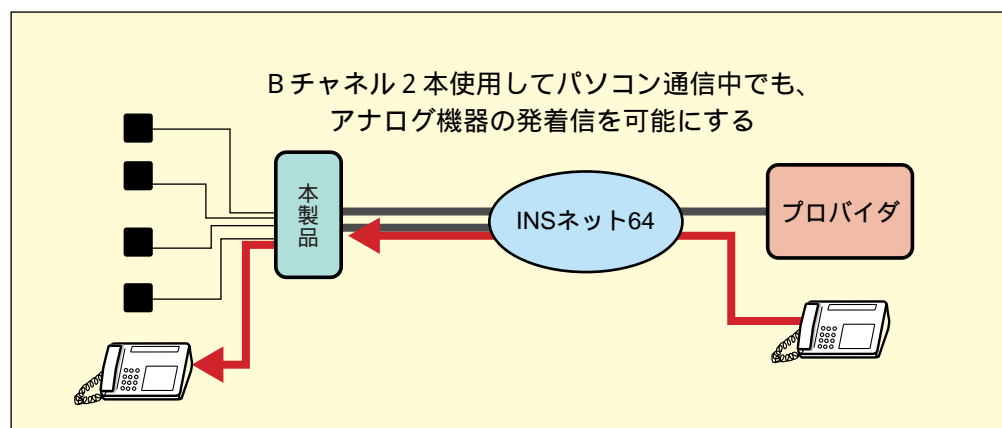
◆UPnP機能を使用しないとき

UPnP機能を使わないときは、［UPnP設定］画面の［UPnP機能］を［OFF］にします。

9 リソースBOD機能を使う

通信中に電話の発信/着信ができるようにする

LANポートにつないだパソコンがBチャネルを2本とも使って通信（MP通信）しているとき、電話機やFAXなどのアナログ機器の発着信をできるようにするか、Bチャネルが空くまでできないようにするかを設定できます。発着信できるようにする機能を「リソースBOD機能」といいます。購入時の設定では、リソースBOD機能を使用する設定になっています。
リソースBOD機能を使用すると、2本のBチャネルでMP通信中に、アナログ機器に発信または着信の要求があると、1本のBチャネルが解放され、アナログ通信に割り当てられます。したがって、アナログの通信を気にすることなく、パソコンで通信をすることができます。

リソースBOD機能を使用するためには、INSネット64の「通信中着信通知サービス」を契約している必要があります（無料）。詳しくは最寄りのNTTまでお問い合わせください。

設定ページ

1. ［詳細設定］をクリックし、［ルータ設定］→［ISDN］をクリックします。
   ［ルータ設定（ISDN）］画面が表示されます。

2. ［リソースBOD（アナログ通信割り込み）］で、次のように設定します。

発信割り込み	許可 ※2本のBチャネルでMP通信していても、アナログ機器から発信できます。データ通信は1本のBチャネルになります。
着信割り込み	許可 ※2本のBチャネルでMP通信していても、アナログ機器に着信できます。データ通信は1本のBチャネルになります。

[リソースBOD(アナログ通信割り込み)]	
発信割り込み	○不許可 ◉許可
着信割り込み	○不許可 ◉許可

※[不許可]を選択すると、MP通信をしているときは、アナログ機器から発信、またはアナログ機器に着信できません。

4. [設定]ボタンをクリックします。

◆本製品のTA機能のリソースBOD機能について

本製品のTA機能でMP通信をしている場合は、リソースBOD（アナログ通信割り込み）機能は使用できません。あらかじめご了承ください。

10 保守

本製品に関する様々な情報を確認する方法を解説します。また、設定内容を保存したり、購入時の状態に戻したり、本製品をバージョンアップする方法なども解説します。必要に応じてお読みください。

時刻を設定する／修正する

本製品は、NTPサーバへアクセスして、本製品の時刻を自動的に修正することができます。自動接続制限を設定しているときは、本機能を利用することをお勧めします。時刻を修正する方法は、次の2通りあります。

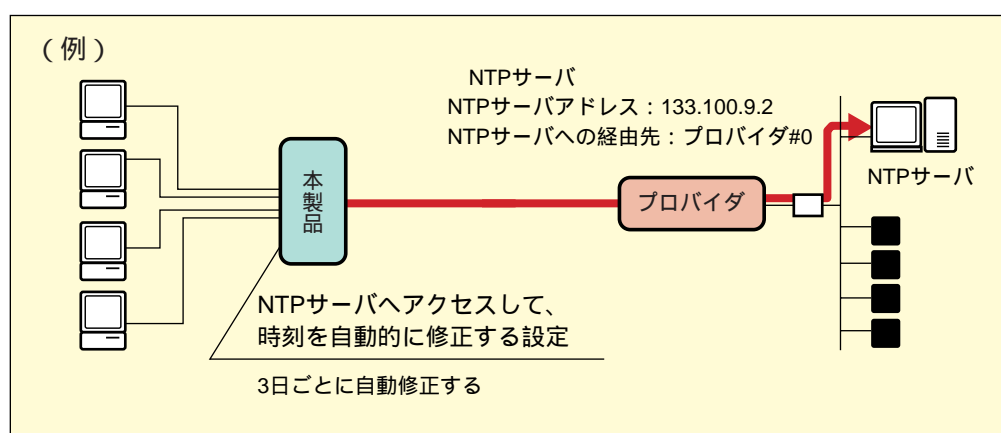
●自動修正

設定された日数間隔ごとにNTPサーバへアクセスして修正します。ただし、NTPサーバが相手先にある場合、設定された日数間隔以降に、その相手先に接続したときに修正します。

※NTPサーバが相手先にある場合でも、自動修正のために本製品が相手先に自動接続することはありません。

※本製品に時刻が設定されていない場合（年が1996の場合）、設定されている日数を経過していなくても、指定した相手先に初めて回線を接続したときに、NTPサーバへ時刻の問い合わせが行われ、自動的に時刻が修正されます。

●手動修正

NTPサーバがある相手先と接続しているとき、あるいは、NTPサーバがLAN上にあるときは、設定ページのボタンを操作すると、ただちにNTPサーバへアクセスして修正できます。

◆本製品の電源をOFFにしたときは日付と時刻を確認してください。
日付と時刻は一度設定しても、本製品の電源をOFFにして24時間経過すると、購入時の設定「1996/01/01-00:00」に戻ります。

設定ページ

1. ［詳細設定］をクリックし、［本体設定］をクリックします。

   ［本体設定］画面が表示されます。

2. ［現在本体に設定されている日付と時刻］を確認し、日付や時刻が違っているときは［設定する日付と時刻］に正しい時刻を入力します。

3. 時刻を自動修正するときは［時刻修正機能］で、次のように設定します。

自動時刻修正	する
NTP サーバアドレス（プライマリ）	133.100.9.2 時刻を確認する1つめのIPアドレスを入力します。 ※「133.100.9.2」は日本の標準時刻を管理している代表的なサーバのIPアドレスです。 ※この項目の入力を省略すると、自動的に「133.100.9.2」と設定されます。
NTP サーバアドレス（セカンダリ）	時刻を確認する2つめのIPアドレスを入力します。省略して構いません。
NTPサーバへの経由先	#0 NTPサーバへアクセスするための経由先を選択します。 ※NTPサーバがLAN上にあるときや、PPPoEを採用していないプロバイダのときは［Ethernet］を選択してください。 ※ISDN、専用線、PPPoEを採用しているプロバイダのときは、#0～#15から相手先を選択してください。
修正する間隔	3 自動修正を行う間隔を入力します。 ※半角１～７文字以内で入力してください。 ※［次回修正予定日時］には、自動時刻修正を行う予定日時が表示されます。

[時刻修正機能]	
自動時刻修正	○しない ⊙する
NTPサーバアドレス(プライマリ)	133.100.9.2
NTPサーバアドレス(セカンダリ)	
NTPサーバへの経由先	#0 プロバイダA
修正する間隔	3 日ごと
次回修正予定日時	1996/01/08-00:54 [今すぐ修正]

4. ［設定］ボタンをクリックします。

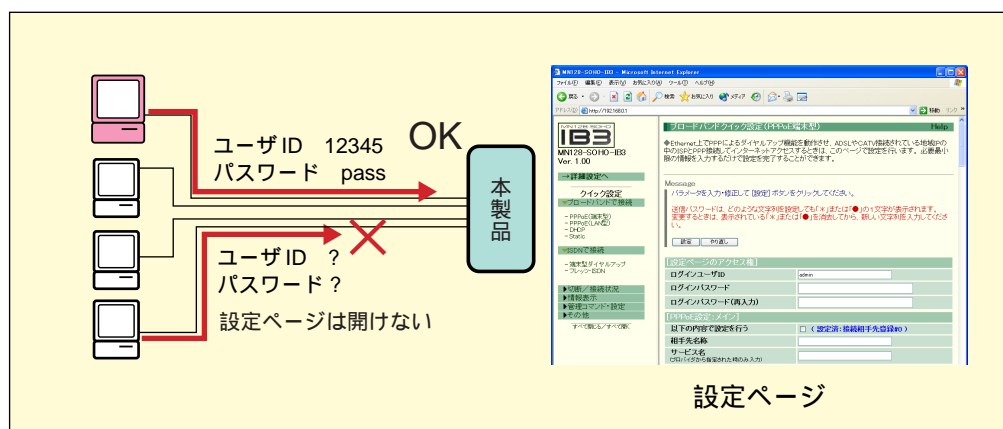
以降、時刻の自動修正が行われます。

手動修正したいときは、［設定］ボタンをクリックしてから［今すぐ修正］ボタンをクリックします。NTPサーバがある相手先と接続しているとき、あるいはNTPサーバがLAN上にあるときは、NTPサーバにアクセスして修正できます。

※［設定］ボタンをクリックせずに［今すぐ修正］ボタンをクリックしても、設定されないので注意してください。

ユーザIDとパスワードを設定する

本製品にユーザIDとパスワードを設定できます。設定したユーザIDとパスワードを知らなければ、本製品の設定ページを開くことができなくなります。ブロードバンドや専用線でインターネットに常時接続する場合は、外部からの侵入を防ぐためにも、必ずこの設定を行ってください。

※クイック設定で、ブロードバンドで接続の各設定、またはフレッツ・ISDNの設定を行う場合にも、ユーザIDとパスワードの設定を行うことができます。

設定ページ

1. ［詳細設定］をクリックし、［管理者コマンド・設定］→［ユーザ・パスワード変更］をクリックします。

   ［管理者コマンド・設定（ユーザ・パスワード変更）］画面が表示されます。

2. 次のように入力します。

ユーザID	12345 ユーザIDを入力します。 ※「no」「clear」は使用できません。
パスワード	pass パスワードを入力します。 ※「no」「clear」「＊（1文字)」「？（1文字)」は使用できません。
パスワード（再入力）	［パスワード］に入力した文字を入力

［ユーザ・パスワード変更］

ユーザID	12345
パスワード	••••
パスワード(再入力)	••••

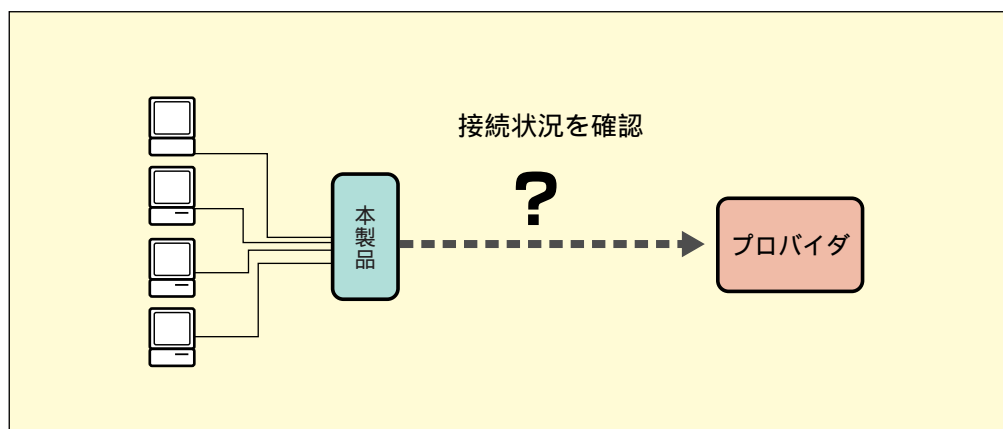
3. ［設定］ボタンをクリックします。

以降、管理者が設定ページを開くときは［パスワード要求］ダイアログで上記で設定した［ユーザID］と［パスワード］を入力してください。また、この設定を行うと、ユーザIDとパスワードを忘れると、設定ページを開くことができません。

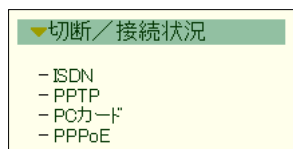
◆ユーザIDとパスワードを忘れたとき
ユーザIDとパスワードを忘れて設定ページが開けなくなった場合は、本製品を初期化して購入時の状態に戻す必要があります。この際、設定した内容がすべて消去されるので、ご注意ください。設定ページが開けないときは、次の方法で本製品を初期化します。

(1) 本体の初期化スイッチを使う→導入/設定ガイド「ルータ機能の設定を購入したときの状態に戻すには」
(2) TELポートの電話機から設定コードを使う→リファレンス・ハンドブック「全設定消去用 ATコマンド・設定コード」
(3) RS-232Cシリアルポートのパソコンから ATコマンドを使う→リファレンス・ハンドブック「全設定消去用ATコマンド・設定コード」

接続状況を確認する

設定ページから、チャネルの使用状況や、接続中の相手先を確認できます。例えば、すでにLANポートにつないだパソコンからインターネットにアクセスしているときは、その回線を使ってほかのパソコンもインターネットにアクセスすることができます。

■PPPoEで接続しているとき/ISDN回線を使用しているとき

設定ページ

1. ［詳細設定（またはクイック設定）］をクリックし、［切断／状況］をクリックします。

2. 接続の状況を確認したい回線やプロトコルなどをクリックします。

接続状況 Help

チャネル	PPPoE1
接続状況	接続中(発信)
接続時刻	2003/09/18 12:32:36
相手先電話番号	PPPoE
接続モード	端末型
リンクプロトコル	LCP IPCP
相手先ルータアドレス	172.16.15.1
相手先DNSサーバアドレス	172.168.0.1
割り当てIPアドレス	172.16.15.2
無通信時間/自動切断時間(秒)	39/なし
経過時間/最大接続時間(分)	25/なし
チャネル	**PPPoE2**
接続状況	空き

※PPPoEをクリックしたときの例です。

現在の接続状況が接続ごとに表示されます。

接続状況	回線が接続されているときは「接続中（発信）」、接続していないときは「空き」と表示されます。 ※着信して接続したときは「接続中（着信）」と表示されます。
接続時刻	接続を開始した時刻が表示されます。
相手先電話番号	［接続／相手先登録］画面の［相手先電話番号］に入力されている電話番号（文字）が表示されます。
接続モード	相手先と接続しているモードに応じて「端末型」または「LAN型」と表示されます。
リンクプロトコル	接続に使用されているプロトコルが表示されます。
相手先ルータアドレス	相手先（プロバイダ）のルータのIPアドレスが表示されます。
相手先DNSサーバアドレス	相手先（プロバイダ）のDNSサーバのIPアドレスが表示されます。
割り当てIPアドレス	端末型接続時に割り当てられる、グローバル IP アドレスが表示されます。 ※接続のたびに違うIPアドレスが割り当てられることがあるので、その都度確認してください。
無通信時間／ 自動切断時間（秒）	通信されていない時間と、設定されている自動切断までの時間が秒単位で表示されます。
経過時間／ 最大接続時間（分）	接続を開始してからの時間と、設定されている最大接続時間が、分単位で表示されます。

ISDNを選択しているときは、「回線使用率（送信/受信/BOD%）」の項目が追加され、回線の利用率が表示されます。

■DHCP接続／固定のIPアドレスでの接続の場合

設定ページ

1. ［詳細設定（またはクイック設定）］をクリックし、［情報表示］→［WAN状況］の順にクリックします。

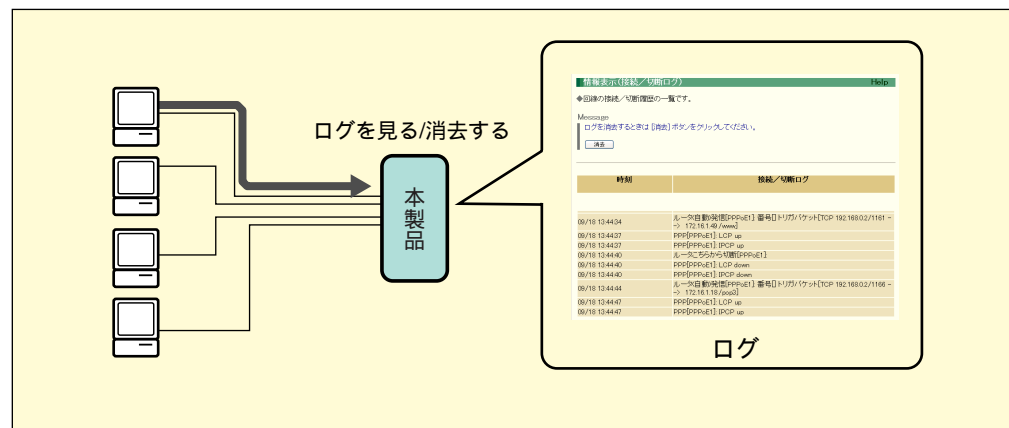
   ［情報表示（WAN状況）］画面が表示されます。

現在の接続状況が表示されます。

MAC アドレス	WANポートのMACアドレスが表示されます。
IPアドレス	接続時に割り当てられるWAN側のグローバルIPアドレス、または手入力したIPアドレスが表示されます。 ※接続時にグローバルIPアドレスが割り当てられる場合、接続のたびに違うIPアドレスが割り当てられることがあるので、その都度確認してください。
サブネットマスク	接続時に割り当てられるサブネットマスク、または手入力したサブネットマスクが表示されます。
デフォルトゲートウェイ	接続時に割り当てられるゲートウェイの IP アドレス、または手入力したゲートウェイの IP アドレスが表示されます。
DNSサーバアドレス	接続時に割り当てられるDNSサーバのIPアドレスが表示されます。
ドメイン名	接続時に割り当てられるドメイン名が表示されます。
DHCPの状態	接続時にWAN側のIPアドレスが割り当てられているときは「取得済み」と表示されます。
リース取得日時	WAN側のIPアドレスが割り当てられた日時が表示されます。
リース取得期限	割り当てられたWAN側のIPアドレスを使用できる期限が表示されます。

接続／切断ログを見る・消去する

本製品を使って通信したときの回線接続ごとの記録をまとめて確認できます。記録は、1時間ごとに本製品のフラッシュメモリに保存されるので、電源をOFFにしても記録は失われません。ただし、記録が257件以上になると古い順に自動的に消去されます。また、記録は手動で消去することもできます。

※フラッシュメモリに保存される前に本製品の電源をOFFにすると、直前までの履歴が保存されない場合があります。

設定ページ

1. ［詳細設定（またはクイック設定）］をクリックし、［情報表示］→［接続／切断ログ］をクリックします。

   ［接続情報（接続／切断ログ）］画面が表示されます。

情報表示（接続／切断ログ） Help

◆回線の接続／切断履歴の一覧です。

Message

ログを消去するときは［消去］ボタンをクリックしてください。

消去

時刻	接続／切断ログ
09/18 13:44:34	ルータ(自動)発信[PPPoE1]: 番号[] トリガパケット[TCP 192.168.0.2/1161 --> 172.16.1.49 /www]
09/18 13:44:37	PPP[PPPoE1]: LCP up
09/18 13:44:37	PPP[PPPoE1]: IPCP up
09/18 13:44:40	ルータこちらから切断[PPPoE1]:
09/18 13:44:40	PPP[PPPoE1]: LCP down
09/18 13:44:40	PPP[PPPoE1]: IPCP down
09/18 13:44:44	ルータ(自動)発信[PPPoE1]: 番号[] トリガパケット[TCP 192.168.0.2/1166 --> 172.16.1.18 /pop3]
09/18 13:44:47	PPP[PPPoE1]: LCP up
09/18 13:44:47	PPP[PPPoE1]: IPCP up

画面には次のような内容が表示されます。

時刻	それぞれの現象が起こった日時が表示されます。
発信に関する情報	発信したチャネルと相手先の電話番号が表示されます。 ※発信に失敗した場合、番号のあとに理由が表示されます。→「設定ページのエラー一覧〈P.124〉」
着信に関する情報	着信したチャネルと相手先の電話番号が表示されます。
切断に関する情報	切断したチャネル、切断理由、こちら側にかかった料金が表示されます。
PPPに関する情報	PPP を使用して接続するときの、相手先とのやりとりの内容が表示されます。

通信料金はダイヤルアップ接続で、次のいずれかに該当する場合だけ表示されます。該当しない場合は、実際に本製品側に通信料金がかかっていても表示されません。

・本製品から接続した回線を本製品が切断したとき
　→接続から切断までにかかった通信料金が表示されます。
・相手先から接続された回線を本製品が切断したとき
　→「0円」と表示されます。

記録が257件以上になると、古い記録は「より過去のログ」画面に表示されます。

次の場合は、ISDN回線から料金情報が通知されないため、［情報表示（接続／切断ログ)］画面に通信料金が「0円」と表示されます。しかし、実際は接続時間に応じた通信料金が本製品側にかかっているので、ご注意ください。

・ PHS電話機に発信した場合
・ 電話をかける際に、「0033（NTTコミュニケーションズ)」「001（KDDI株式会社)」「0088（日本テレコム株式会社)」などの番号を付けた場合
・ PHS電話機を利用した機器にPIAFSで発信した場合
・ PHS電話機を利用した機器からアクセス（PIAFS）を受信した際に、本製品からコールバックした場合
・ 本製品に接続したFOMA/PHS/モデムの対応PCカードから発信した場合

なお、ブロードバンドをご利用の場合は接続時間に応じた通信料金が必要無いので、通信料金は「0円」と表示されています。

2. 記録を消去する場合は、［消去］ボタンをクリックします。

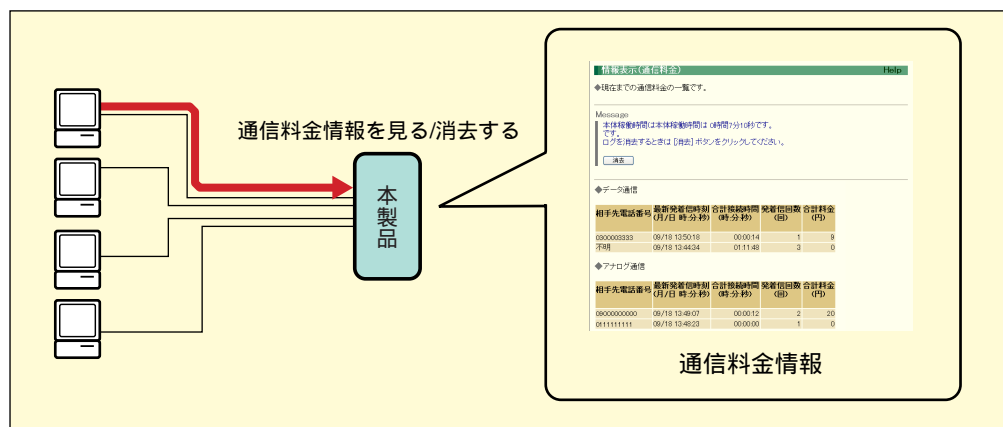
とくに必要がない限り、通常は消去しないでください。

◆［情報表示（接続／切断ログ)］画面に正しい日付と時刻を表示させる

正しい日付や時刻を確認するためには、［本体設定］の［設定する日付と時刻］に正しい日付や時刻を設定してください。なお、本製品の電源をOFFにしてから24時間経過すると、購入時の設定「1996/01/01-00：00」に戻ります。購入時の設定に戻ったときは、改めて正しい日付と時刻を入力してください。→「時刻を設定する／修正する」〈P.81〉

◆SYSLOGサーバ機能に対応しているパソコンでログ情報を一括管理
［情報表示（接続／切断ログ）］画面の記録やデバック情報、フィルタリング情報（本製品に設定しているフィルタに該当した発着信の情報）を、SYSLOGサーバ機能に対応しているパソコンに転送して、ファイルとして一括管理できます。
SYSLOGサーバを利用するときは、［ルータ設定（LAN）］画面で行います。詳しくは、活用ガイド中・上級編「SYSLOGサーバに出力する」を参照してください。

通信料金情報を見る／消去する

端末型ダイヤルアップ接続で、本製品から相手先に接続したときの接続時間の合計や通信料金の合計などを、相手先の電話番号ごとに確認できます。また、これらの情報を消去することもできます。

設定ページ

1. **［詳細設定（またはクイック設定）］をクリックし、［情報表示］→［通信料金］をクリックします。**

   ［接情報表示（通信料金）］画面が表示されます。

   ※ブロードバンドをご利用の場合は、相手先電話番号が「不明」、料金が「0円」で表示されます。

情報表示（通信料金）　Help

◆現在までの通信料金の一覧です。

Message
本体稼働時間は本体稼働時間は 0時間7分10秒です。
です。
ログを消去するときは［消去］ボタンをクリックしてください。

消去

◆データ通信

相手先電話番号	最新発着信時刻（月/日 時:分:秒）	合計接続時間（時:分:秒）	発着信回数（回）	合計料金（円）
0300003333	09/18 13:50:18	00:00:14	1	9
不明	09/18 13:44:34	01:11:48	3	0

◆アナログ通信

相手先電話番号	最新発着信時刻（月/日 時:分:秒）	合計接続時間（時:分:秒）	発着信回数（回）	合計料金（円）
09000000000	09/18 13:49:07	00:00:12	2	20
0111111111	09/18 13:48:23	00:00:00	1	0

相手先電話番号	相手先の電話番号が表示されます。
最新発着信時刻	各相手先に、一番最近発着信した時刻が表示されます。
合計接続時間	各相手先に接続した時間の合計が表示されます。
発着信回数	相手先に接続した回数の合計が表示されます。 ※発信したけれど話し中だった、アナログ機器に着信があったけれど受話器を上げなかった、など通信料金がかからなかった場合も、回数がカウントされます。
合計料金	各相手先との通信料金が表示されます。

2　情報を消去する場合は、［消去］ボタンをクリックします。

ネットワークやパソコンの設定内容や運用によっては、回線が接続されたままになったり、意図していない自動接続を行うことがあります（例えば、一部のWebサイトでは、サーバから情報を送り続けるものがあります）。お客様の意図していない接続については、弊社は一切責任を負いかねますので、あらかじめご了承ください。本製品の導入後しばらくは、接続状況や通信料金に特にご注意ください。

- 本体ランプ→ISDN回線に接続中はB1またはB2ランプが点灯します。ブロードバンドで接続中は、WANランプ・PPPoEランプが点灯します。
  ※設定によっては、PPPoEランプは点灯しません。
- 設定ページの［接続状況］画面→現在接続されている回線の状況が確認できます。
- 設定ページの「情報表示（通信料金）」画面→最新の発着信の状況などを確認できます。

次の環境では本製品を使用しないように注意してください。

- すでに稼働しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行うように設定しないでください。
- LANポートにつないだパソコンで、定期的にISDN回線を接続して通信を行うソフトウェアを起動したままにしないでください。

また、LAN上のパソコンが、意図していない自動接続を行うことがあります。そのときは、［接続／切断］画面で、自動接続のきっかけとなったパケット（トリガパケット）を確認してトリガパケットを出しているパソコンの設定を確認してください。あるいは、［ルータ設定（LAN）］画面でトリガパケットを破棄するためのフィルタを設定してください。フィルタについて詳しくは、活用ガイド中・上級編「IPフィルタの設定」を確認してください。

次の場合は、ISDN回線から料金情報が通知されないため、［情報表示（接続／切断ログ）］画面に通信料金が「0円」と表示されます。しかし、実際は接続時間に応じた通信料金が本製品側にかかっているので、ご注意ください。

- **PHS電話機に発信した場合**
- **電話をかける際に、「0033（NTTコミュニケーションズ）」「001（KDDI株式会社）」「0088（日本テレコム株式会社）」などの番号を付けた場合**
- **PHS電話機を利用した機器にPIAFSで発信した場合**
- **PHS電話機を利用した機器からアクセス（PIAFS）を受信した際に、本製品からコールバックした場合**
- **本製品に接続したFOMA/PHS/モデムの対応PCカードから発信した場合**

なお、ブロードバンドをご利用の場合は、接続時間に応じた通信料金が必要ではないので、「0」円と表示されます。

◆日付と時刻が正しいかどうか確認してください。

設定ページの［本体設定］→［設定する日付と時刻］で1日に1度は日付や時刻を確認してください。一度設定しても、本製品の電源をOFFにしてから24時間経過すると、購入時の設定「1996/01/01-00：00」に戻ります。購入時の設定に戻ったときは、改めて正しい日付と時刻を入力してください。→**「時刻を設定する／修正する」〈P.81〉**

1ヶ月ごとの通信料金情報を見る

通信料金の情報を自動的に消去する日を設定することによって、1ヶ月単位で通信料金を見ることができます。月に一度、設定した日の午前0時（00:00）になると［情報表示（通信料金)］画面に表示される情報が自動的に消去されます。消去された情報は「先月分」として1ヶ月間保存されます。通信料金の情報は、今月分・先月分ともに64件まで保存できます。64件を超えた場合は、通信料金の安い順に自動的に消去されます。

設定ページ

1. ［詳細設定］をクリックし、［本体設定］をクリックします。
［本体設定］画面が表示されます。

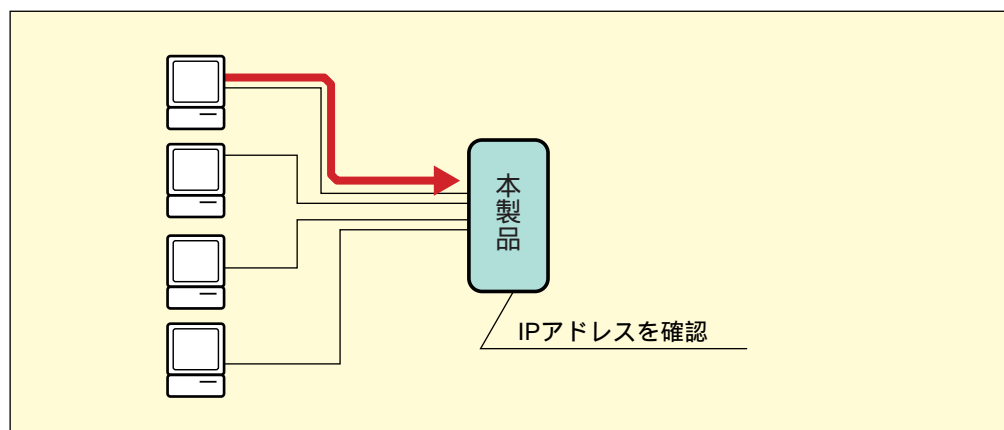
2 ［スケジュール機能］の項目で、次のように設定します。

通信料金情報の消去	する
消去する日	消去する日を入力 （入力した日の 00:00 に消去されます。）

［スケジュール機能］	
通信料金情報の消去	○しない ◉する
消去する日	毎月 1 日

◆先月分の通信料金がすでにある場合、［通信料金設定の消去］を［する］から［しない］に変更すると、先月分の情報が消去されます。
◆［通信料金］画面の［消去］ボタンをクリックすると、今月分と先月分の両方の情報がすべて消去されます。
◆表示される通信料金は、あくまでも目安です。実際の請求金額と異なる場合があります。

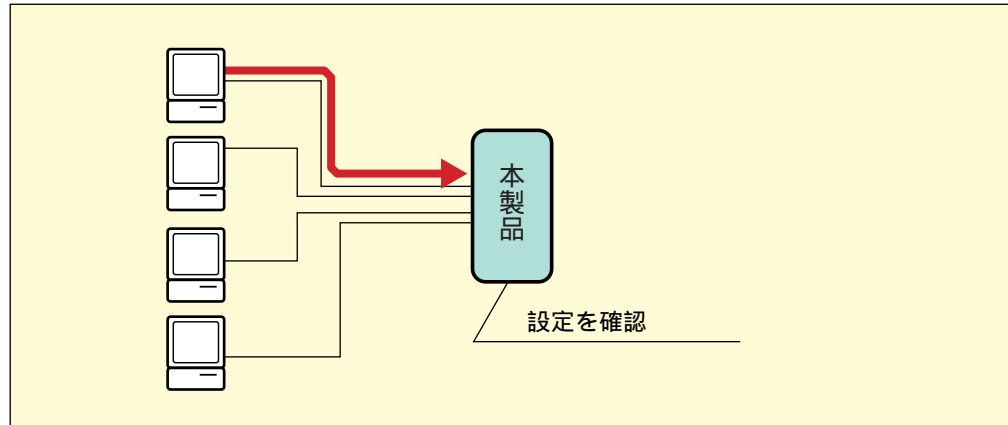
本製品のIPアドレスを確認する

本製品のIPアドレスは、設定ページの［ルータ設定（LAN）］画面で確認できます。

設定ページ

1. ［詳細設定］をクリックし、［ルータ設定］→［LAN］をクリックします。

   ［ルータ設定（LAN）］画面が表示されます。［本体のIPアドレス/サブネットマスク長］を確認してください。

設定を確認する

［情報表示（設定）］画面では、本製品のルータ機能に関する設定をまとめて確認できます。

設定ページ

1. **［詳細設定（またはクィック設定）］をクリックし、［情報表示］→［設定］をクリックします。**

   ［情報表示（設定）］画面が表示されます。

   ※下記の図は、表示例です。

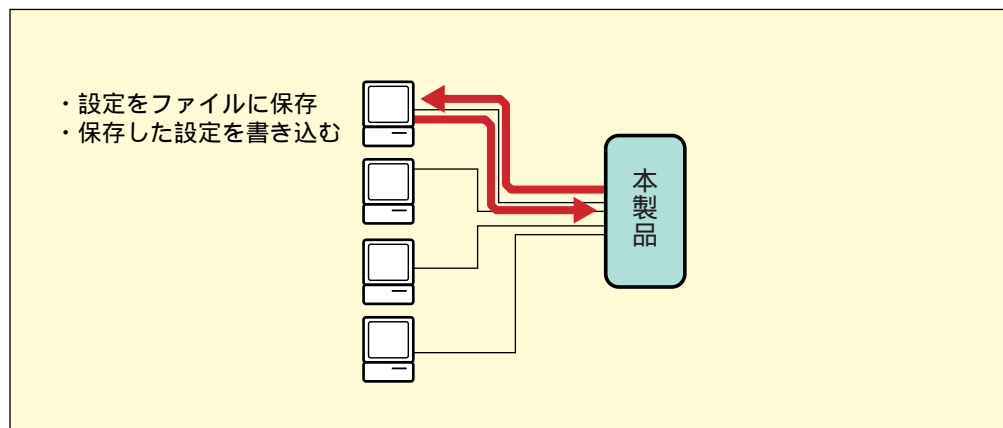
```
# MN128-SOHO IB3 1.00   Oct 17 2003 10:27:06
# MAC Address: 00:00:00:80:d1:54
sys encrypt e1faea9fd5283df8
card air11 ssid MN8021180D154
ip address 192.168.0.1/24
ip dhcp server on
ip filter 45 reject in 10.0.0.0/8 * * * * remote 0
ip filter 46 reject in 172.16.0.0/12 * * * * remote 0
ip filter 47 reject in 192.168.0.0/16 * * * * remote 0
ip filter 48 reject in 10.0.0.0/8 * * * * remote 1
ip filter 49 reject in 172.16.0.0/12 * * * * remote 1
ip filter 50 reject in 192.168.0.0/16 * * * * remote 1
ip filter 51 reject out * 10.0.0.0/8 * * * remote 0
ip filter 52 reject out * 172.16.0.0/12 * * * remote 0
ip filter 53 reject out * 192.168.0.0/16 * * * remote 0
ip filter 54 reject out * 10.0.0.0/8 * * * remote 1
ip filter 55 reject out * 172.16.0.0/12 * * * remote 1
ip filter 56 reject out * 192.168.0.0/16 * * * remote 1
ip filter 57 reject in * 192.168.0.1/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany
ip filter 60 reject dns qtype 6
ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany
ip route 0.0.0.0/0/7 remote 0,1 auto
remote 0 channel pppoeled
```

購入時の設定から変更した内容が表示されます。

◆［情報表示（設定）］画面でのパスワードの表示

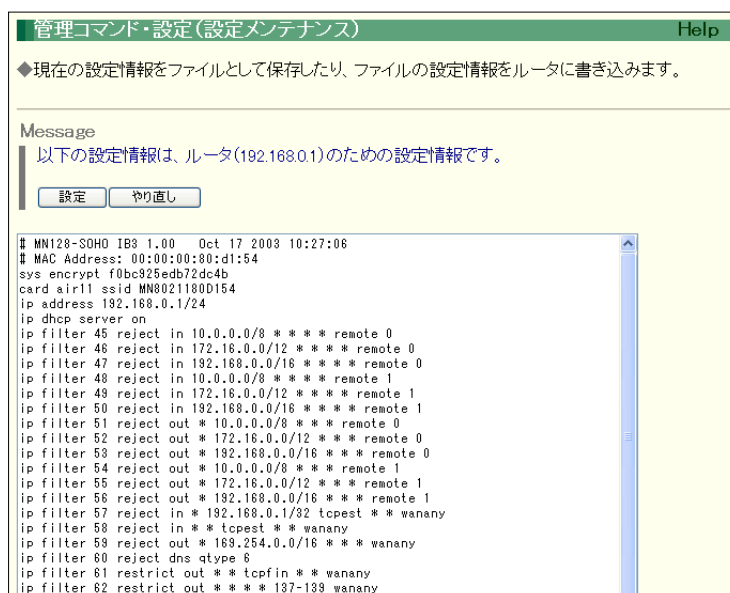
［情報表示（設定）］画面では、パスワード、メールパスワード、鍵配送鍵を暗号化したコード（暗号コード）で表示します。暗号コードは、各設定ページで設定を行うごとに更新されます。

設定をファイルに保存する／保存した設定を書き込む

設定ページで設定した内容を、HTML形式のファイルに保存できます。設定をファイルに保存しておくと、別のMN128-SOHO IB3に同じ設定をするときや、何らかのトラブルで本製品の設定内容が失われたときなどに利用できます。なお、設定を保存したファイルを「設定ファイル」といいます。

■設定を保存するとき

設定ページ

1. ［詳細設定］をクリックし、［管理コマンド・設定］→［設定メンテナンス］をクリックします。

   ［管理コマンド・設定（設定メンテナンス）］画面が表示されます。

画面のテキストボックスには、現在の設定がコマンド一覧で表示されています。
※テキストボックス内の文字を、削除したり変更しないでください。

2. Webブラウザの［ファイル］メニューから［名前を付けて保存］や［別名で保存］など、ファイル名を付けて保存するためのコマンドを選択します。

   ファイル名を入力するためのダイアログが表示されます。

3. ファイル名を入力します。

   Windowsでは［ファイルの種類］で［Webページ、完全（*.htm;html）］を、Macintoshでは［形式］で［HTMLソース］を選択します。

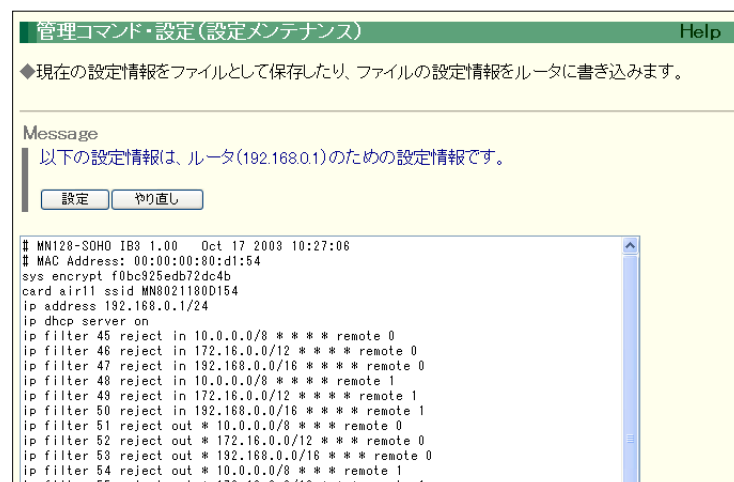
   ※保存ファイルのエンコードを選択できるWebブラウザの場合は、［シフトJIS］を選択してください。

4. 保存を実行します。

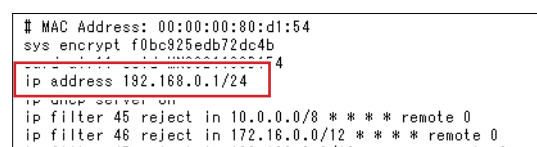
   設定ページの内容が、ファイルに保存されます。

■設定内容を本製品に書き込むとき

1. Webブラウザの［ファイル］メニューから［開く］などのコマンドで設定ファイルを開きます。

   設定ファイルの内容が、Webブラウザのウィンドウに表示されます。

2. 設定ファイル内の、本製品のIPアドレスを確認します。

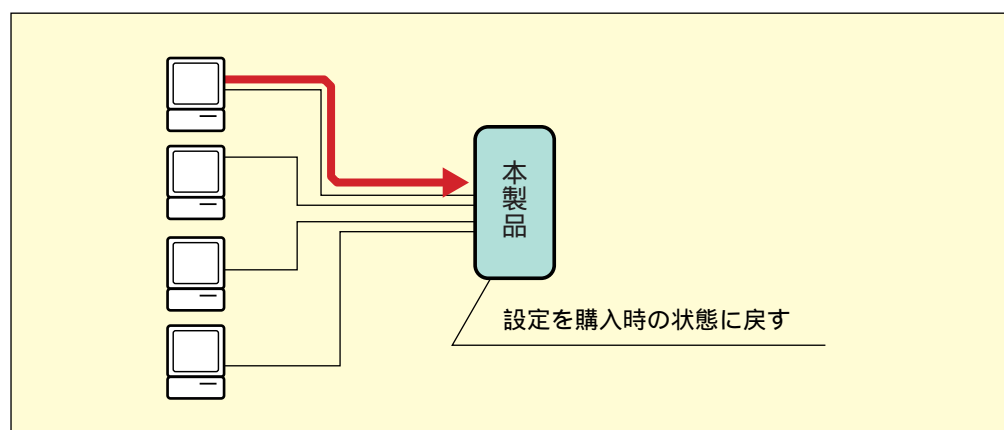
   表示されているIPアドレスが、設定を書き込むMN128-SOHO IB3のIPアドレスと異なる場合は、表示されているIPアドレスを修正して、設定を書き込むMN128-SOHO IB3のIPアドレスに直します。

```
# MAC Address: 00:00:00:80:d1:54
sys encrypt f0bc925edb72dc4b
ip address 192.168.0.1/24
ip filter 45 reject in 10.0.0.0/8 * * * * remote 0
ip filter 46 reject in 172.16.0.0/12 * * * * remote 0
```

   ※その他の項目は変更しないでください。

3. ［設定］ボタンをクリックします。

   「設定が終了しました。」というメッセージが表示されます。設定ファイルの内容が書き込まれます。

設定を購入時の状態に戻す

本製品の設定内容を消去して、購入時の設定に戻すことができます。本製品のIPアドレスも、購入時の設定「192.168.0.1」に戻ります。
なお、設定内容を消去する前に、あらかじめ現在の設定内容をファイルに保存しておくことをお勧めします。操作方法については「設定をファイルに保存する／保存した設定を書き込む」〈P.98〉を参照してください。

設定ページ

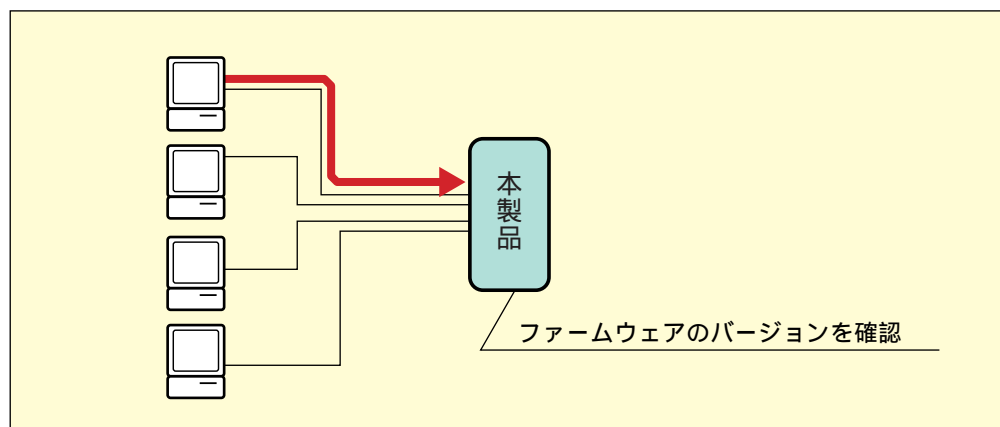
1. ［詳細設定（またはクイック設定）］をクリックし、［管理コマンド・設定］→［設定の消去］をクリックします。
   ［管理コマンド・設定（設定の消去）］画面が表示されます。

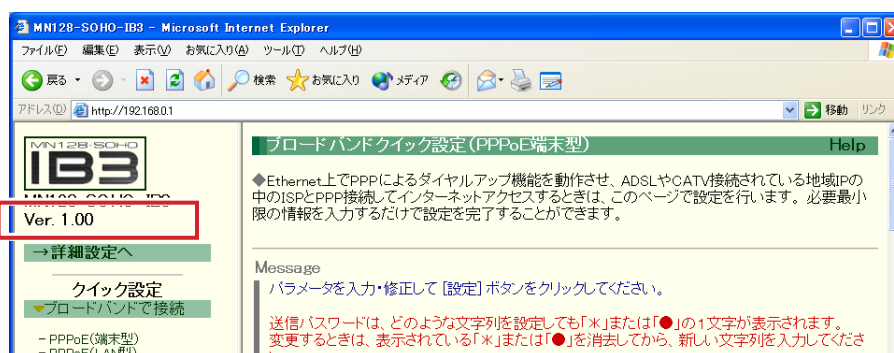
2. ［消去する設定情報］で、消去する項目を選択します。
   ［すべての設定］を選択すると、設定したすべての内容が購入時の内容に戻ります。
   ※接続・切断ログ、通信料金情報、着信メール一覧は［すべての設定］を選択しても消去されません。それぞれの画面で消去を実行してください。

3. ［消去］ボタンをクリックします。

4. 本製品を再起動します。

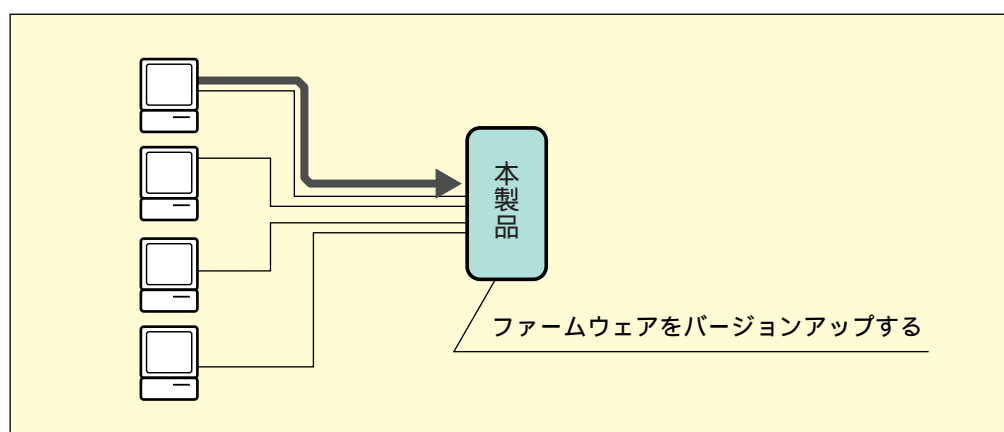
本製品のファームウェアのバージョンを確認する

本製品のファームウェアは、不定期にバージョンアップを行っています。お使いのファームウェアのバージョンを確認する方法を解説します。

設定ページ

1. **本製品のLANポートにつないだパソコンから設定ページを開くと、画面左側にファームウェアのバージョンが表示されます。**

◆ファームウェアのアップデートについて
本製品の最新のファームウェアは、MN128-SOHOのホームページで入手できます。また、ファームウェアのアップデートは専用のツールを使用して行います。詳しくは、「本製品をバージョンアップする」〈P.102〉をお読みください。

本製品をバージョンアップする

本製品の最新のファームウェアはMN128-SOHOホームページから、無料でダウンロードできます。定期的にMN128-SOHOホームページにアクセスして最新のファームウェアを入手し、本製品をバージョンアップ（アップデート）してください。ダウンロードしたファームウェアのアップデートは、本製品のLANポートにつないだパソコンから、アップデータを使って行います。

※RS-232Cシリアルポートのパソコンからもバージョンアップできますが、その場合別途シリアルケーブル（D-sub9pin（メス-メス）ストレート全結線ケーブル）をご用意ください。

◆あらかじめ設定内容を保存しておくことをお勧めします。

アップデータは、自動的に本製品の設定内容を保存し、ファームウェアのアップデート後にもとの設定を書き込みますが、安全のため、アップデートを実行する前には設定を保存しておいてください。→「設定ファイルを保存する／保存した設定内容を書き込む」〈P.98〉

パソコンの設定

1. **Webブラウザを起動して、MN128-SOHOホームページにアクセスします。**

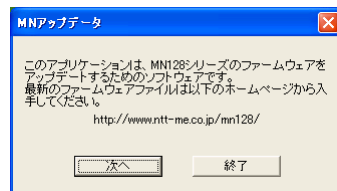
   ●MN128-SOHOホームページのURL
   株式会社エヌ・ティ・ティ エムイー：http://www.ntt-me.co.jp/mn128/

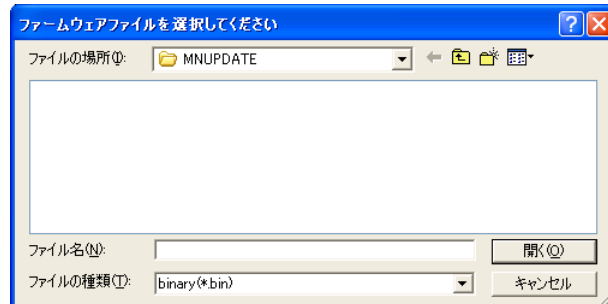
2. **バージョンアップ方法のページを表示します。**

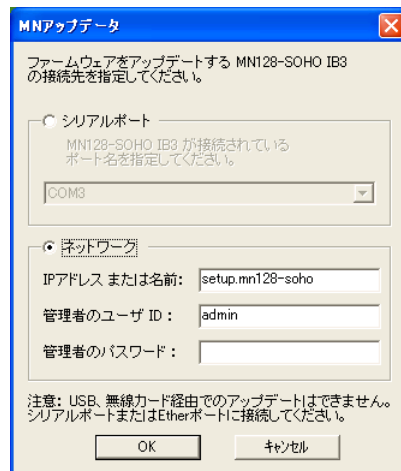
3. **ページの指示に従って、最新のアップデータとファームウェアをダウンロードします。**

   ※端末型ダイヤルアップ接続でインターネットにアクセスしている場合は、ダウンロードが終了したらすべての回線を切断してください。

4. **アップデータを、本製品のLANポートにつないだパソコンにインストールします。**

5　アップデータを起動します。

6　［次へ］ボタンをクリックします。

ファームウェアファイルを選択するダイアログが表示されます。

7　ファームウェアファイルを選択し、［開く］ボタンをクリックします。

本製品の接続先を指定するダイアログが表示されます。

8　接続先を選択します。

●本製品がパソコンのRS-232Cシリアルポートに接続されているとき

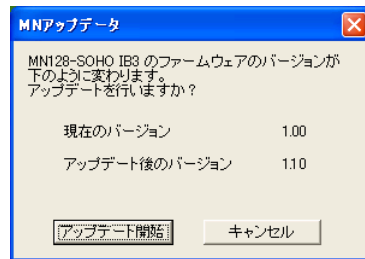
［シリアルポート］をクリックし、ポートを指定します。

●本製品がLAN上にあるとき

［ネットワーク］をクリックし、本製品のIPアドレスを入力します。ユーザIDとパスワードが設定されているときは、設定しているユーザIDとパスワードを入力します。

※ユーザIDとパスワードを設定していないときは、［ユーザID］に［admin］、［パスワード］は空欄にしておきます。

9　［OK］ボタンをクリックします。

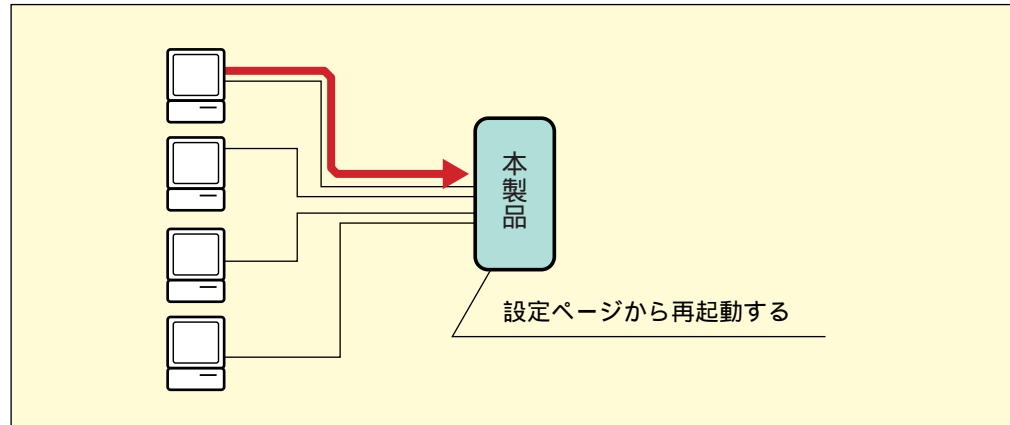
ファームウェアのバージョンが表示されます。

10［アップデート開始］ボタンをクリックします。

設定を保存するかどうか確認する画面が表示されます。
設定を保存する場合は［はい］ボタンを、保存しない場合は［いいえ］ボタンをクリックしてください。

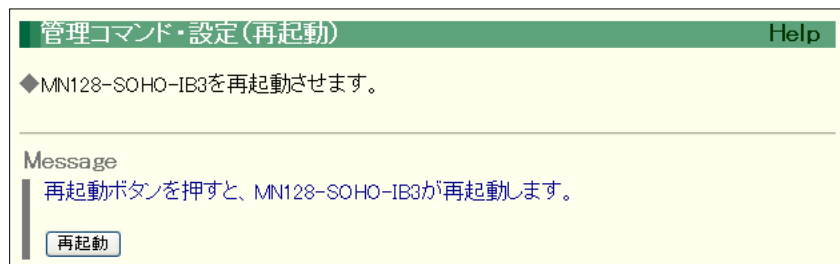
※どちらかのボタンをクリックしなければ、アップデートが開始されません。

アップデートが始まります。
アップデートが終了したら、アップデータを終了します。

本製品を再起動する

設定ページから本製品を再起動できます。

設定ページ

1. **［詳細設定（またはクイック設定)］をクリックし、［管理コマンド・設定］→［再起動］をクリックします。**

   ［管理コマンド・設定（再起動)］画面が表示されます。

2. **［再起動］ボタンをクリックします。**

   しばらくすると、本製品が再起動します。

活用ガイド～初級編

付録

ここでは、おもに本製品を使用しているときのトラブル対処方法についてまとめています。困ったこと、わからないことがでてきたときにお読みください。

1. 困ったときは ··108
2. 設定ページのエラー一覧 ································124
3. クイック設定で自動的に設定されるフィルタ ··········131
4. お問い合わせ先 ·······································138
5. 用語解説 ···140

1 困ったときは

本製品が正常に動作しない場合は、該当する項目を確認してください。

ISDN、FOMA/PHS/モデムの対応PCカードのトラブル

■発着信できない

→［情報表示（接続／切断ログ）］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.124〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→［接続／相手先登録］画面の［相手先電話番号］が正しいか確認してください。

→［接続／相手先登録］画面の［送信ユーザID］が正しいか確認してください。

→［接続／相手先登録］画面の［送信パスワード］が正しいか確認してください。

→［接続／相手先登録］画面の［認証プロトコル］が正しいか確認してください。

→［接続／相手先登録］画面の［通信チャネル］が正しいか確認してください。

→発信は、３分間に３回だけ可能です。３分経過してから、もう一度発信してください。

→相手先に次のことを確認してください。

・ほかの通信機器が応答していませんか？
・各機器は正しく接続していますか？
・着信を許可していますか？

■自動接続できない

→［自動接続相手先］画面で自動接続する相手を変更しませんでしたか？

自動接続したい相手先を選択してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定していると、［自動接続可能な時間帯］しか自動接続できません。

→［情報表示（自動接続制限）］画面を確認してください。［再接続制限］欄に「禁止」と表示されている場合は、料金制限、回数制限、最大接続時間経過後の自動接続の制限のいずれかによって、自動接続を禁止されています。次のように対処してください。

- ［情報表示（自動接続制限）］画面で、自動接続を禁止している制限項目をリセットしてください。
- 料金制限、回数制限によって自動接続を禁止されている場合は、［接続相手先登録］画面の［料金による制限］（料金制限の場合）あるいは［接続回数による制限］（回数制限の場合）の数値を増やして、再設定してください。

→［情報表示（接続／切断ログ）］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.124〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→ ［ルータ設定（LAN)］画面の［オプション］に、自動接続のためのIP経路情報が正しく登録されているか確認してください。

→ ［情報表示（IP経路)］画面で自動接続先のルート（「mode」が「auto」と表示されているルート）が正しいか確認してください。

→ ［接続／相手先登録］画面から手動で相手先に接続できるか確認してください。

→ ［ルータ設定（LAN)］画面の［オプション］に登録されているフィルタ、IPアドレス変換テーブルやソース経路情報が正しいかどうか確認してください。

→ Windows XP/2000/98 SE/Meで自動接続できない場合は、次の原因が考えられます。

Windows XP/2000/98 SE/Me/を使用している場合、その仕様により、意図しない自動接続が発生してしまうことがあります。そのため、本製品では、購入時にあらかじめ次のフィルタが登録されています。

```
ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany
```

※フィルタ番号は、上記と異なる場合があります。

また、Windows 2000 Serverのドメインに所属するパソコンが、Microsoftネットワークにログオンする場合、Windows 2000 Serverと通信して、ログオン名とパスワードの認証を受けます。その際、Windows 2000 Serverが遠隔地にあるときは、上記のフィルタのために回線を自動接続することができません。
Microsoftネットワークにログオンするときや、共有フォルダへアクセスするときなどに、回線を自動接続したい場合は、［ルータ設定（LAN)］画面の［オプション］に登録されている上記のフィルタを削除してください。
ただし、これらのフィルタを削除すると、Windows XP/2000/98 SE/Meが遠隔地のワークグループまたはドメインに所属する場合、マスタブラウザへ定期的にアクセスするため、回線の自動接続が発生しますので、ご注意ください。

→ Windows 2000 Serverが自動接続できない場合は、次の原因が考えられます。

Windows 2000 Serverは、電源投入時にパソコンのIPアドレスをDNSサーバに登録する機能があります。そのため、本製品のAutoDNS機能を使用している場合には、パソコンの電源を入れると自動接続を行います。この自動接続を防ぐために、あらかじめ購入時の本製品には、次のフィルタが登録されています。

```
ip filter 60 reject dns qtype 6
```

※フィルタ番号は、上記と異なる場合があります。

LAN上のWindows2000 ServerでIPアドレスをDNSサーバに登録したいときなどに、回線を自動接続したい場合は、［ルータ設定（LAN)］画面の［オプション］に記載されている上記のフィルタを削除してください。
ただし、上記のフィルタを削除すると、LAN上にWindows 2000 Serverがある場合、自動接続が発生します。ご注意ください。

■勝手に接続してしまう

→ LAN上にWindows XP/2000/98 SE/Me/があるとき、意図しない自動接続が行われていることがあります。

通常、Windows XP/2000/98 SE/Meを接続しているルータを自動接続するように設定すると、意図的に通信操作を行わなくても、定期的に（約15秒ごと）自動接続してしまいます。これは、Windows XP/2000/98 SE/Meの仕様のために発生します。
この自動接続を防ぐために、あらかじめ本製品には、購入時の設定で次のフィルタが登録されています。

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

※フィルタ番号は、上記と異なる場合があります。

・ip filter 61
パソコン上でWWWブラウザを終了するときに送信される、不要なパケットによる自動接続を防止するためのフィルタです。なお、「tcpfin」はTCPのセッションによる終了時のTCPパケットだけを対象にします。

・ip filter 64
指定のポートを使用する、自動接続のきっかけとなるパケット（トリガパケット）を破棄するためのフィルタです。なお、手動で接続したときや、すでに回線が接続されているときは、指定のポートを使用して通信を行うことができます。
フィルタは、［ルータ設定（LAN）］画面の［オプション］で確認・削除することができます。
ただし、次のケースに当てはまる場合は、Windows XP/2000/98 SE/Meで設定を行う必要があります。

▼ケース1
WindowsのTCP/IPの設定で、相手先のDNSサーバアドレスを指定している、または、AutoDNS機能を使用し本製品にLAN側のDNSサーバアドレスを指定していない場合
●Windows XP/2000
［インターネットプロトコル（TCP/IP）のプロパティ］を開きます。［詳細設定］ボタンをクリックして［TCP/IP詳細設定］ダイアログを開き、次のように設定します。
・［DNS］タブで［この接続のアドレスをDNSに登録する］のチェックを外す
・［WINS］タブで［NetBIOS over TCP/IPを無効にする］を選択
●Windows 98 SE/Me
特別な設定は必要ありません。

▼ケース2
WindowsのTCP/IPの設定でLAN側のDNSサーバアドレスを指定している、または、AutoDNS機能を使用し、本製品にLAN側のDNSサーバアドレスを設定している場合

●Windows XP/2000
［インターネットプロトコル（TCP/IP）のプロパティ］を開きます。［詳細設定］ボタンをクリックして［TCP/IP詳細設定］ダイアログを開き、次のように設定します。
・［DNS］タブで［この接続のアドレスをDNSに登録する］のチェックを外す
・［WINS］タブで［NetBIOS over TCP/IPを無効にする］を選択

●Windows 98 SE/Me
DNSサーバを使用しないように設定します。
しかし、Windows98 SE/Meは、ホスト名やワークグループ名の問い合わせを解決するために、必ずDNSサーバを使用する仕様になっています。そのため、コントロールパネルで設定を変更することができません。
したがって、DNSサーバを使用しないように設定するには、レジストリと呼ばれるシステムのデータベースを直接書き換えてください。レジストリの書き換え方法は、マイクロソフト社の「Knowledge Base」と呼ばれるサポート用データベースに記載されているので（Article ID:Q137368）、米マイクロソフト社のホームページなどから参照できます。
なお、レジストリに関する操作は、システムクラッシュなどの危険が伴いますので、十分注意しながら行ってください。詳しくは、パソコンのマニュアルなどを参照してください。

▼その他
ほかにも、意図しない自動接続が行われてしまうことがあります。その場合は、自動接続のきっかけとなったパケット（トリガパケット）を確認し、送信元のパソコンの設定を見直してください。または、そのトリガパケットを破棄し、意図しない自動接続が行われないようにするためのフィルタを設定してください。

●自動接続の原因となる通信を行っているパソコンを限定する
1.［情報表示（接続／切断ログ）］画面を開きます。
2.「ルータ発信」という項目で、「トリガパケット」という文字が入っているログを探します。

```
ルータ（自動発信）［B1］：番号［0300001234］トリガパケット［UDP 192.168.0.3/ntp
-->172.16.0.129/ntp
```

この例では、「192.168.0.3のパソコンが、172.16.0.129のパソコンにUDP（ntp）の通信を行おうとして自動接続が起きた」ということを表しています。
この場合、192.168.0.3のパソコンの設定を確認してください。

●限定されたパソコンが自動接続を行わないようにフィルタを設定する
1.［ルータ設定（LAN）］画面を開きます。
2.［オプション］欄で、フィルタを設定します。

```
ip filter 1 restrict out 192.168.0.3 * udp ntp ntp remote *
```

この例は、192.168.0.3のパソコンが、172.16.0.129のパソコンにUDP（ntp）の通信を行おうとして自動接続が起きている場合に設定するフィルタです。
※フィルタについて詳しくは、活用ガイド～中・上級編「IPフィルタの設定」を参照してください。

ケース1、ケース2の場合、Microsoftネットワークを使用して相手先のWindows XP/2000/98 SE/Me/の共有フォルダを利用できなくなります。これは、購入時のフィルタや上記の設定によって、ホストのIPアドレスの問い合わせを解決できなくなるためです。
この場合は、活用ガイド～中・上級編「Windows間で共有フォルダを利用する」に従って設定してください。
本製品を簡易DNSサーバとして使うときに、LAN上のパソコンのホスト名を登録しておくと、そのパソコンへアクセスする際、相手先に自動接続してしまうことはありません。活用ガイド～中・上級編「簡易DNSサーバにする」を参照してください。

→ LAN上にWindows 2000があるとき、意図しない自動接続が行われてしまうことがあります。この自動接続を防ぐために、Windows 2000側または本製品側で設定をする必要があります。

▼Windows 2000側で設定するとき

1. ［コントロールパネル］→［ネットワークとダイヤルアップ接続］を開き、［ローカルエリア接続］を右クリックしてプロパティを開きます。
   ［ローカルエリア接続のプロパティ］ウィンドウが開きます。
2. ［インターネットプロトコル（TCP/IP)］をリストから選択し、［プロパティ］ボタンをクリックします。
   ［インターネットプロトコル（TCP/IP）のプロパティ］ウィンドウが開きます。
3. ［詳細設定］ボタンをクリックします。
   ［TCP/IP詳細設定］ウィンドウが開きます。
4. ［DNS］タブの［DNSドメイン名］の下に［この接続のアドレスをDNSに登録する］のチェックを外します。
5. ［OK］ボタンをクリックします。
   手順2～4で開いたウィンドウをすべて閉じます。

▼本製品側で設定するとき

1. ［ルータ設定（LAN)］画面を開きます。
2. ［AutoDNS機能］をONにします。
3. DNS Queryパケットに関するIPフィルタを登録します。
   ip filter N reject dns qtype 6
   ※Nには1～64までの数字を入力します。
   ※クィック設定を行うと、「ip filter 60 reject dns qtype 6」が設定されます。
   ※すべての設定を消去すると、自動的にこのフィルタが登録されます。
4. ホスト情報にローカルエリア接続のドメイン名を登録します。
   ip host xxx.xxx.xxx.xxx ###
   ※「xxx.xxx.xxx.xxx」には、LAN内で使用していないIPアドレスを、「###」には、Windows2000に設定しているドメインまたはワークグループを入力してください。ドメインやワークグループは、［マイコンピュータ］→［ネットワークID］タブの［詳細設定］で確認できます。
5. ［設定］ボタンをクリックします。

ネットワークの設定内容や運用によっては、長時間、回線が接続したままになることや意図していない自動接続が行われていることがあります。初期導入後は、必ず［切断／接続状況］画面、［情報表示（通信料金）］画面を確認してください。

■相手先と通信できない

→ パソコンのTCP/IPの設定が正しいか確認してください。

- パソコンのIPアドレスとサブネットマスクを正しく設定していますか？
- ゲートウェイを正しく設定していますか？
- DNSサーバのIPアドレスを正しく設定していますか？

→ 端末型ダイヤルアップ接続する場合、［切断／接続状況］画面の［割り当てIPアドレス］でIPアドレスを取得しているか確認してください。

→ フィルタ（［ルータ設定（LAN）］画面の［オプション］で設定）を正しく登録しているか確認してください。

→ 相手先によっては、AutoDNS機能が正常に働かないことがあります。

接続する相手先が設定されている［接続／相手先登録］画面の［DNSサーバアドレス］に、相手先のDNSサーバのIPアドレスを入力してください。

→ ご使用の通信ソフトの設定を確認してください。

プロキシサーバを正しく指定していますか？

→ 相手先が他社のルータを使用している場合、スタティックルートの設定が必要なことがあります。（活用ガイド中・上級編「固定したルート（スタティックルート）で通信する（WAN側）」参照）

→ LAN型ダイヤルアップ接続する場合、次のことを確認してください。

- こちら側のLANと相手先のLANに、異なるサブネットワーク番号を使用してください。
- numbered接続のときは、WAN側のIPアドレスの設定が必要です。→活用ガイド～中・上級編「numbered接続する」を参照
- numbered接続するときは、WAN側のサブネットマスクの設定が必要なことがあります。→活用ガイド～中・上級編「numbered接続する」を参照

■データ通信中に回線が切断されてしまう

→ ［情報表示（接続／切断ログ）］画面でどちら側から切断したのかを確認してください。

「こちらから切断」と表示されているときは、以下を参照して対処してください。
「相手先から切断」と表示されているときは、相手先に問い合わせてください。

→ ［接続／相手先登録］画面の［自動切断タイマ１］を設定していると、設定した時間、回線上で通信がなかったときは自動的に回線が切断されます。自動切断を止めたいときは、［自動切断タイマ１］に「0」を設定してください。

この場合、接続したら必ず手動で切断してください。

特に次の環境で本製品を使用しないように注意してください。
- **すでに稼動しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行う設定にしているとき**
- **LAN上のパソコンで定期的に回線を接続して通信を行うソフトウェアを起動しているとき**

※［切断／接続状況］画面や［情報表示（通信料金）］画面で、回線の使用状況や通信料金を確認してください。

これらの画面について詳しくは「接続状況を確認する」〈P.86〉「通信料金情報を見る／消去する」〈P.92〉をそれぞれ参照してください。

→［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［タイマ２の時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［最大接続時間］を設定していないか確認してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［自動接続可能な時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［時間帯による着信制限］を「以下の時間帯のみ着信許可」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［着信を許可する時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

■自動切断しない

→［接続／相手先登録］画面の［自動切断タイマ1］を「0」に設定していると自動切断しません。

→［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」、かつ、［自動切断タイマ2］を「0」に設定していると、［タイマ２の時間帯］は自動切断しません。

→ 相手先と通信が行われていないか確認してください。

→ LAN上のすべての機器の電源をOFFにする、あるいは、LAN上の各機器のケーブルをすべて外してみてください。自動切断する場合は、LAN上の機器が相手先と通信している可能性があります。LAN上の各機器の設定を確認してください。

すべての機器を外しても切断しないときは、相手からパケットが送信されている可能性があります。その場合は、自動切断せずに必ず手動で切断してください。

→ 本製品が受信したパケットによって、［自動切断タイマ1/2］がリセットされ、自動切断ができなくなることがあります。

なお、次のパケットの場合は、リセットされません。
（1）Echo 、EchoReply以外のICMPパケット
　ICMPパケットではリセットされません。ただし、pingではリセットされます。

（2）ブロードキャストUDPパケット
Destinationアドレスがすべて1、またはホスト部がすべて1のパケットではリセットされません。

（3）以下のサービスのUDPポート
Destinationポートが以下のパケットではリセットされません。
RIP（520）、NTP（123）、RWHO（513）、AT_ZIS（206）、ATLS（216）、SUNRPC（111）、　BOOTPC（68）、BOOTPS（67）、KIP（200..205）

（4）DNAME検索のUDPパケット
Sourceポート番号、またはDestinationポート番号がDNAME（53）のパケットでは、リセットされません。

（5）PPTP（1723）のTCPパケット
PPTPパケットではリセットされません。

（6）GRE（プロトコル番号47）のKeepAliveパケット
PPTP接続後GREプロトコルによって行われるKeepAliveパケットではリセットされません。
また、GREパケット内に含まれるIPパケットの内容が（1）～（4）に該当する場合は、リセットされません。

■本製品同士で接続できない

→ 発信側の場合、［ルータ設定（ISDN）］画面の［ISDN番号*サブアドレス］に、相手先に通知する電話番号（自分側の電話番号）を設定してください。本製品を購入時の設定のまま使用していると、［ISDN番号*サブアドレス］にはサブアドレス「1」が設定されているため、相手先にサブアドレス付きの番号が通知され、着信できないことがあります。

→ 着信側の場合、［情報表示（接続／切断ログ）］画面で相手に通知された電話番号を確認し、それと同じ電話番号を［接続／相手先登録］画面の［相手先電話番号］に設定してください。

■FTPソフトでファイルの送受信ができない

→次のように、FTPソフトの設定を「PASVモード」に変更してください。

・Windows用　NextFTP（Ver.1.91）の場合
［オプション］→［ファイヤーウォール（プロキシ）］タブで［PASVモード］をチェックします。

・Macintosh用　Fetch（Ver.3.0.3J2）の場合
［初期設定］→［Firewall］で［パッシブモード転送（PASV）を使う］をチェックします。

※FTPによるデータ転送は、通常、サーバ側からクライアント側へアクセスした後にデータ転送を開始する仕組みになっています。しかし、本製品の購入時の設定では、外部からの不正なアクセスを防止するため、WAN側から本製品へのアクセスができないようになっています。そのため、FTPサーバからクライアント側へのアクセスもできません。「PASVモード」とは、この現象を回避するため、クライアント側からサーバ側へアクセスするようにした転送方法です。

■Windows Messenger / MSN Messengerで通信できない

→ 本製品とWindows XP/MeのUPnPの設定を確認してください。Messengerを利用するときは、本製品とWindows XP/MeともにUPnP機能をONする必要があります。

●本製品のUPnP設定をONにする

1. ［詳細設定］→［UPnP設定］をクリックし、［UPnP機能］を［ON］にします。

●Windows XPのUPnP設定をONにする

1. ［スタート］メニューの［コントロールパネル］をクリックし、［ネットワーク接続］をクリックします。
   ［ネットワーク接続］ウィンドウが表示されます。
2. ［詳細設定］メニューから［オプションネットワークコンポーネント］を選択します。
3. コンポーネントの一覧で［ネットワークサービス］をクリックし、［詳細］ボタンをクリックします。
4. ［ネットワークサービス］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows XPの画面の指示に従ってください。

●Windows MeのUPnP設定をONにする

1. ［スタート］メニューの［設定］から、［コントロールパネル］をクリックします。
2. ［アプリケーションの追加と削除］アイコンをダブルクリックして、［Windowsファイル］タブをクリックします。
3. ［コンポーネントの種類］で［通信］をクリックし、［詳細］ボタンをクリックします。
4. ［コンポーネントの種類］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows Meの画面の指示に従ってください。

→ 通信相手の動作環境を確認してください。通信相手がUPnP対応のルータを使用していますか？または、プライベートIPアドレスを使用しているプロバイダ経由で接続していませんか？このような場合は、Messengerで通信できません。

→ Messengerでの通信がなくなってから、本製品のUPnPポート自動削除設定で設定した時間が経過したときは、自動的に使用されていたポートが閉じます。ポートが閉じてから再びMessengerを使いたいときは、Messengerをいったん終了してから、起動し直してください。Messengerでサインインし直すだけでは正常に動作しませんので ご注意ください。

ブロードバンドのトラブル

■ブロードバンド接続ができない

→「情報表示（接続/切断ログ）」画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.124〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→「接続／相手先登録」画面の「送信ユーザID」が正しいか確認してください。

→「接続／相手先登録」画面の「送信パスワード」が正しいか確認してください。

→「接続／相手先登録」画面の「認証プロトコル」が正しいか確認してください。

→「接続／相手先登録」画面の「暗号化」が正しいか確認してください。

→ ブロードバンド接続には、「PPPoE（端末型）」「PPPoE（LAN型）」「DHCP」「Static」の異なる設定方法があります。プロバイダの契約（接続形態）と設定している画面が一致していますか？

→ 本製品前面のWANのランプを確認してください。

点灯していない場合は、ケーブルが外れているか、ケーブルが切断されている場合があります。

→ PPPoEランプを確認してください。

クイック設定でPPPoEを設定した場合、もしくは 詳細設定で通信チャネルを「PPPoE（ランプ点灯）」で設定した場合は、PPPoEランプが点灯します。点灯しない場合は「送信ユーザID」「送信パスワード」などの設定を再確認してください

→ プロバイダの工事は終了していますか？

契約を申し込んでから、工事が完了するまで日数がかかる場合があります。申し込んだプロバイダに確認してください。

→ クイック設定をしたあと、別のクイック設定をしませんでしたか？

「クイック設定」ページの［PPPoE（端末型)］、［PPPoE（LAN型］［端末型ダイヤルアップ］［フレッツ・ISDN］の各画面は、詳細設定ページの「接続/相手先登録」画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■ブロードバンド回線で再接続できない

→ ケーブルを抜いたり、正常に切断処理をしないで本装置の電源を切った場合にはしばらく（数分間）再接続できないことがあります。しばらくたってから再接続してみてください。

■自動接続できない

→［自動接続相手先］画面で自動接続する相手を変更しませんでしたか？

自動接続したい相手先を選択してください。

→ ［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定していると、［自動接続可能な時間帯］しか自動接続できません。

→ ［情報表示（自動接続制限）］画面を確認してください。［再接続制限］欄に「禁止」と表示されている場合は、料金制限、回数制限、最大接続時間経過後の自動接続の制限のいずれかによって、自動接続を禁止されています。次のように対処してください。

- ［情報表示（自動接続制限）］画面で、自動接続を禁止している制限項目をリセットしてください。
- 料金制限、回数制限によって自動接続を禁止されている場合は、［接続相手先登録］画面の［料金による制限］（料金制限の場合）あるいは［接続回数による制限］（回数制限の場合）の数値を増やして、再設定してください。

→ ［情報表示（接続／切断ログ）］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.124〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→ ［ルータ設定（LAN）］画面の［オプション］に、自動接続のためのIP経路情報が正しく登録されているか確認してください。

→ ［情報表示（IP経路）］画面で自動接続先のルート（「mode」が「auto」と表示されているルート）が正しいか確認してください。

→ ［接続／相手先登録］画面から手動で相手先に接続できるか確認してください。

→ ［ルータ設定（LAN）］画面の［オプション］に登録されているフィルタ、IPアドレス変換テーブルやソース経路情報が正しいかどうか確認してください。

→ Windows XP/2000/98 SE/Meで自動接続できない場合は、次の原因が考えられます。

Windows XP/2000/98 SE/Me/を使用している場合、その仕様により、意図しない自動接続が発生してしまうことがあります。そのため、本製品では、購入時にあらかじめ次のフィルタが登録されています。

```
ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany
```

※フィルタ番号は、上記と異なる場合があります。

また、Windows 2000 Serverのドメインに所属するパソコンが、Microsoftネットワークにログオンする場合、Windows2000 Serverと通信して、ログオン名とパスワードの認証を受けます。その際、Windows2000 Serverが遠隔地にあるときは、上記のフィルタのために回線を自動接続することができません。
Microsoftネットワークにログオンするときや、共有フォルダへアクセスするときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に登録されている上記のフィルタを削除してください。
ただし、これらのフィルタを削除すると、Windows XP/2000/98 SE/Meが遠隔地のワークグループまたはドメインに所属する場合、マスタブラウザへ定期的にアクセスするため、回線の自動接続が発生しますので、ご注意ください。

→ Windows 2000 Serverが自動接続できない場合は、次の原因が考えられます。

Windows 2000 Serverは、電源投入時にパソコンのIPアドレスをDNSサーバに登録する機能があります。そのため、本製品のAutoDNS機能を使用している場合には、パソコンの電源を入れると自動接続を行います。この自動接続を防ぐために、あらかじめ購入時の本製品には、次のフィルタが登録されています。

ip filter 60 reject dns qtype 6

※フィルタ番号は、上記と異なる場合があります。

LAN上のWindows 2000 ServerでIPアドレスをDNSサーバに登録したいときなどに、回線を自動接続したい場合は、[ルータ設定（LAN)] 画面の [オプション] に記載されている上記のフィルタを削除してください。
ただし、上記のフィルタを削除すると、LAN上にWindows2000 Serverがある場合、自動接続が発生します。ご注意ください。

■相手先と通信できない

→ パソコンのTCP/IPの設定が正しいか確認してください。

- パソコンのIPアドレスとサブネットマスクを正しく設定していますか？
- ゲートウェイを正しく設定していますか？
- DNSサーバのIPアドレスを正しく設定していますか？

→ 端末型ダイヤルアップ接続する場合、[切断／接続状況] 画面の [割り当てIPアドレス] でIPアドレスを取得しているか確認してください。

→ フィルタ（[ルータ設定（LAN)] 画面の [オプション] で設定）を正しく登録しているか確認してください。

→ 相手先によっては、AutoDNS機能が正常に働かないことがあります。

接続する相手先が設定されている [接続／相手先登録] 画面の [DNSサーバアドレス] に、相手先のDNSサーバのIPアドレスを入力してください。

→ ご使用の通信ソフトの設定を確認してください。

プロキシサーバを正しく指定していますか？

→ 相手先が他社のルータを使用している場合、スタティックルートの設定が必要なことがあります。(活用ガイド中・上級編「固定したルート（スタティックルート）で通信する（WAN側)」参照)

→ LAN型ダイヤルアップ接続する場合、次のことを確認してください。

- こちら側のLANと相手先のLANに、異なるサブネットワーク番号を使用してください。
- numbered接続のときは、WAN側のIPアドレスの設定が必要です。→活用ガイド～中・上級編「numbered接続する」を参照
- numbered接続するときは、WAN側のサブネットマスクの設定が必要なことがあります。→活用ガイド～中・上級編「numbered接続する」を参照

■データ通信中に回線が切断されてしまう

→［情報表示（接続／切断ログ）］画面でどちら側から切断したのかを確認してください。

「こちらから切断」と表示されているときは、以下を参照して対処してください。
「相手先から切断」と表示されているときは、相手先に問い合わせてください。

→［接続／相手先登録］画面の［自動切断タイマ１］を設定していると、設定した時間、回線上で通信がなかったときは自動的に回線が切断されます。自動切断を止めたいときは、［自動切断タイマ１］に「0」を設定してください。

この場合、接続したら必ず手動で切断してください。

特に次の環境で本製品を使用しないように注意してください。
・すでに稼動しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行う設定にしているとき
・LAN上のパソコンで定期的に回線を接続して通信を行うソフトウェアを起動しているとき
※［切断／接続状況］画面や［情報表示（通信料金）］画面で、回線の使用状況や通信料金を確認してください。
これらの画面について詳しくは「接続状況を確認する」〈P.86〉「通信料金情報を見る／消去する」〈P.92〉をそれぞれ参照してください。

→［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［タイマ２の時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［最大接続時間］を設定していないか確認してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［自動接続可能な時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［時間帯による着信制限］を「以下の時間帯のみ着信許可」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［着信を許可する時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

■FTPソフトでファイルの送受信ができない

→次のように、FTPソフトの設定を「PASVモード」に変更してください。

・Windows用　NextFTP（Ver.1.91）の場合
［オプション］→［ファイヤーウォール（プロキシ）］タブで［PASVモード］をチェックします。
・Macintosh用　Fetch（Ver.3.0.3J2）の場合
［初期設定］→［Firewall］で［パッシブモード転送（PASV）を使う］をチェックします。

※FTPによるデータ転送は、通常、サーバ側からクライアント側へアクセスした後にデータ転送を開始する仕組みになっています。しかし、本製品の購入時の設定では、外部からの不正なアクセスを防止するため、WAN側から本製品へのアクセスができないようになっています。そのため、FTPサーバからクライアント側へのアクセスもできません。「PASVモード」とは、この現象を回避するため、クライアント側からサーバ側へアクセスするようにした転送方法です。

■Windows Messenger / MSN Messengerで通信できない

→ 本製品とWindows XP/MeのUPnPの設定を確認してください。Messengerを利用するときは、本製品とWindows XP/MeともにUPnP機能をONする必要があります。

●本製品のUPnP設定をONにする

1. ［詳細設定］→［UPnP設定］をクリックし、［UPnP機能］を［ON］にします。

●Windows XPのUPnP設定をONにする

1. ［スタート］メニューの［コントロールパネル］をクリックし、［ネットワーク接続］をクリックします。
   ［ネットワーク接続］ウィンドウが表示されます。
2. ［詳細設定］メニューから［オプションネットワークコンポーネント］を選択します。
3. コンポーネントの一覧で［ネットワークサービス］をクリックし、［詳細］ボタンをクリックします。
4. ［ネットワークサービス］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows XPの画面の指示に従ってください。

●Windows MeのUPnP設定をONにする

1. ［スタート］メニューの［設定］から、［コントロールパネル］をクリックします。
2. ［アプリケーションの追加と削除］アイコンをダブルクリックして、［Windowsファイル］タブをクリックします。
3. ［コンポーネントの種類］で［通信］をクリックし、［詳細］ボタンをクリックします。
4. ［コンポーネントの種類］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows Meの画面の指示に従ってください。

→ 通信相手の動作環境を確認してください。通信相手がUPnP対応のルータを使用していますか？または、プライベートIPアドレスを使用しているプロバイダ経由で接続していませんか？このような場合は、Messengerで通信できません。

→ Messengerでの通信がなくなってから、本製品のUPnPポート自動削除設定で設定した時間が経過したときは、自動的に使用されていたポートが閉じます。ポートが閉じてから再びMessengerを使いたいときは、Messengerをいったん終了してから、起動し直してください。Messengerでサインインし直すだけでは正常に動作しませんのでご注意ください。

その他のトラブル

■相手先の設定が勝手に変わってしまう

→［クイック設定］ページの［PPPoE（端末型）］画面、［PPPoE（LAN型）］画面、［端末型ダイヤルアップ］画面、［フレッツ・ISDN］画面は、［詳細設定］ページの［接続／相手先登録］画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■メール着信通知機能で自動確認が行われなくなった

→［メール設定（着信メール一覧）］画面に表示されるエラーを「[メール設定（着信メール一覧）］画面のエラー」から探し、必要な処置を行ってください。

→［メール設定（着信メール一覧）］画面の［メール確認］ボタンをクリックして、正しくメールが確認されているかどうか、確認してください。

→ 自動接続が制限されていると、メールの自動確認は行われません。

■パソコンを再起動すると「IPアドレスが使えない」というメッセージが表示される

→［ルータ設定（LAN）］画面の［DHCPサーバ機能］をONにしていますか？

→［ルータ設定（LAN）］画面の［開始IPアドレス/個数］で、Ethernet上の機器より少ない個数を設定していませんか？

→ DHCPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定していますか？

固定する場合、ホスト情報に登録するパソコンのIPアドレスを、DHCPサーバ機能で割り当てることができる範囲内（[ルータ設定（IP設定）］画面の［開始IPアドレス/個数]）で設定してください。

■本製品と通信できない／設定ができない

→パソコンのTCP/IPの設定が正しいか確認してください。（活用ガイド～中・上級編「既存のLAN環境で使用する　(1) 購入時のIPアドレスのまま導入する」「既存のLAN環境で使用する　(2) 本製品のIPアドレスを変更して導入する」参照）

- パソコンのIPアドレスとサブネットマスクは正しく設定していますか？
- パソコンのIPアドレスは、本製品のIPアドレスと同じサブネットワーク番号で設定していますか？
- ゲートウェイは正しく設定されていますか？
- DNSサーバのIPアドレスは正しく設定されていますか？

→ Webブラウザの［オプション］メニューなどで、「プロキシサーバ（あるいはプロクシ）を使用しない」ように設定してください。

- 使用しているWebブラウザの設定で「必要時にインターネットに接続する」などの項目を選択していませんか？

・ 使用しているWebブラウザの設定で「プロキシサーバー経由で接続する」などの項目を選択していませんか？

→ WebブラウザのURLを指定する欄に、「http://［本製品のIPアドレス］/」を入力して設定ページを開いてみてください。

開くことができない場合は、パソコンでのIPアドレスの設定が正しいか確認してください。（活用ガイド～中・上級編「既存のLAN環境で使用する （1）購入時のIPアドレスのまま導入する」、「既存のLAN環境で使用する （2）本製品のIPアドレスを変更して導入する」参照）

→ 設定ページで設定するときにエラーが表示されていないか確認してください。

→ お使いのパソコンがWindowsの場合は、MS-DOSプロンプト画面などでpingを入力して、パソコンと本製品が正しくIP通信しているかどうか確認してください。

→ ルータ機能に関する設定を消去して、最初から設定し直してみてください。詳しくは、「設定を購入時の状態に戻す」〈P.100〉を参照してください。

→ ファームウェアを再アップデートしてください。（「本製品をバージョンアップする」〈P.102〉を参照）

■本製品の設定をファイルとして保存できない

→ 設定ファイルを保存するとき、ファイルを保存するダイアログでファイルの種類を［HTML］や［HTMLソース］などを選択して保存しましたか？

設定ファイルは、HTML形式にしてください。

■設定ファイルの設定内容を本製品に書き込めない

→ ［本体設定］画面の［本体の名称］の設定を変更したあとで、パソコンを再起動しましたか？

本製品の名前を変更した場合、本製品の名前で設定ファイルを読み込むためには、パソコンを再起動する必要があります。

→ 設定ファイルが壊れている可能性があります。

■設定したパスワードを忘れてしまった

→ 本体のリセットスイッチを使って、ルータ機能の設定を購入時の状態に戻してください。詳しくは、導入／設定マニュアル「ルータ機能の設定を購入時の状態に戻すには」を参照してください。

2 設定ページのエラー一覧

［接続／相手先登録］画面から手動で相手先に接続しようとした場合にエラーメッセージが表示されたときや、［情報表示（接続／切断ログ）］画面にエラーが表示されているときは、下記を参照して対処してください。

MN128-SOHO ISDN網エラー

●［網理由表示＃６：チャネル利用不可］

→ 相手先がISDN回線を使用しているか確認してください。

●［網理由表示＃17：着ユーザビジー］

→ 相手先のISDN回線のBチャネルが空いていません。しばらく待ってから、再発信してください。

●［網理由表示＃18：着ユーザレスポンスなし］

→ 相手先が応答しません。
［接続相手先登録］画面の［相手先電話番号］を確認してください。

→ 相手先の端末が正しく接続されているか確認してください。

●［網理由表示＃20：加入者不在］

→ しばらく待ってから、再発信してください。

→ 相手先が応答しません。
［接続／相手先登録］画面の［相手先電話番号］を確認してください。

●［網理由表示＃21：通信拒否］

→ 相手先に接続を拒否されました。
相手先が着信を許可しているか確認してください。

●［網理由表示＃27：相手端末故障中］

→ 相手先に次のことを確認してください。
・端末の電源をONにしていますか？
・各機器を正しく接続していますか？

●［網理由表示＃28：無効番号フォーマット（不完全番号）］

→ ［接続／相手先登録］画面の［相手先電話番号］を確認してください。

●［網理由表示＃34：利用可回線／チャネルなし］

→ ほかの端末によって使用されているため、こちら側のISDN回線のBチャネルが空いていません。Bチャネルが空いてから、再発信してください。

●［網理由表示＃41：一時的障害］

→ しばらく待ってから、再発信してください。

●［網理由表示＃44：要求回線／チャネル利用不可］

→ 相手先のISDN回線のBチャネルが空いていません。相手先のBチャネルが空いてから、再発信してください。

●［網理由表示＃88：端末属性不一致］

→ 相手先の属性が異なります。
相手先と属性が一致しているか確認してください。

→ 電話機やファクシミリなどが応答しました。
［接続／相手先登録］画面の［相手先電話番号］を確認してください。

→ 相手先に次のことを確認してください。
・各機器は正しく接続していますか？
・各機器にサブアドレスを正しく設定していますか？

MN128-SOHO PPPエラー

●［PPPエラー：認証プロトコル不一致］

→［接続／相手先登録］画面の［認証プロトコル］を変更して、再発信してください。

●［PPPエラー：認証失敗］

→ IDまたはパスワードが間違っています。
［接続／相手先登録］画面の［送信ユーザID］［送信パスワード］に正しいIDおよびパスワードを設定して、再発信してください。

→ 暗号化の設定が間違っています。
・MPPEで暗号化したデータをやり取りする場合は、［接続／相手先登録］画面で次の設定を確認してください。
［認証プロトコル］は［MS-CHAPv2］を選択する
［暗号化］で［MPPE-40］または［MPPE-128］のどちらかを選択（双方で同じものを選択してください。）なお、どちらかで［MPPE-any］を選択しても構いません。

・本製品独自の暗号化したデータをやり取りする場合は、双方で［接続／相手先登録］画面の［暗号化］を「独自」、［鍵配送鍵］に同じ文字列を設定して、再発信してください。

●［PPPエラー：接続要求再送タイムアウト］

→ 本製品を再起動して、再発信してください。

●［PPPエラー：認証再送タイムアウト］

→ 本製品を再起動して、再発信してください。

●［PPPエラー：プロトコル拒否］

→ 本製品を再起動して、再発信してください。

→ 相手先がIP通信をサポートしていない場合があります。
相手先の通信プロトコルを確認してください。

●［PPPエラー：コールバック要求失敗］

→ コールバックできません。
［接続／相手先登録］画面の［コールバック発信］で［なし］を選択してください。

●［PPPエラー：割り当てIPアドレスなし］

→ リモートアクセスを受ける側の場合は、［ルータ設定（LAN）］画面の［リモートアクセスサーバ機能］を［ON］に、リモートアクセスを許可する側の場合は、［リモートIPアドレス1/2/3/4］にリモートアクセス用のIPアドレスを設定してください。

→ こちらから発信したときにこのメッセージが表示される場合は、次のことを確認してください。
- 相手先はリモートアクセスを許可していますか？
- 相手先を登録している［接続／相手先登録］画面の［接続モード］で［端末型接続］を選択してください。

●［PPPエラー：LCP接続要求再送タイムアウト］

→［接続／相手先登録］画面の［通信チャネル］を変更してください。

●［PPPエラー：LCP接続失敗］

→［接続／相手先登録］画面の［通信チャネル］を変更してください。

●［PPPエラー：CBCP不許可］

→ コールバックできません。
［接続／相手先登録］画面の［コールバック発信］で［なし］を選択してください。

● ［PPPエラー：IPCP接続要求再送タイムアウト］

→［接続／相手先登録］画面の［接続モード］を変更してください。

→相手先がIPプロトコルをサポートしているか、確認してください。

● ［PPPエラー：IPCP接続失敗］

→［接続／相手先登録］画面の［接続モード］を変更してください。

→相手先がIPプロトコルをサポートしているか、確認してください。

［メール設定（着信メール一覧）］画面のエラー

●エラー1：メールサーバ（SMTPサーバ）と通信できませんでした。

→パソコンからメールソフトなどを使って、ネットワークやメール（POP、SMTP）サーバが正しく動作しているかどうか確認してください。

●エラー2：転送先メールアドレスが正しくありません。

→［メール設定（メール着信通知設定）］画面の［転送先メールアドレス］が正しく設定されているかどうか確認してください。

●エラー3：SMTPコマンドがタイムアウトしました。

→パソコンからメールソフトなどを使って、ネットワークやメール（POP、SMTP）サーバが正しく動作しているかどうか確認してください。

●エラー4：その他のエラー

→［メール設定（メール着信通知設定）］画面の［転送元メール（SMTP）サーバ］［転送先メールアドレス］が正しく設定されているかどうか確認してください。

→パソコンからメールソフトなどを使って、ネットワークやメール（POP、SMTP）サーバが正しく動作しているかどうか確認してください。

●接続エラー1（相手先への接続失敗、相手先設定等を確認してください）

→回線ビジー、番号間違いなどの理由で接続できませんでした。以降も、メールの自動確認は継続して行われます。

●接続エラー1（自動接続制限されています）

→［メール設定（メール着信通知設定）］画面の［接続する相手先］で設定している相手先が自動接続制限されているため接続できませんでした。以降も、メールの自動確認は継続して行われます。

●接続エラー1（着ユーザビジー）

→ 相手先の回線がビジーのため接続できませんでした。以降も、メールの自動確認は継続して行われます。

●接続エラー1（空きチャネルなし）

→ 自分側のBチャネルが空いていないため、接続できませんでした。以降も、メールの自動確認は継続して行われます。

●接続エラー1（再発信規制）

→ 再発信規制のため、接続できませんでした。3分以内に3回以上の発信はできません。しばらく待ってから再発信してください。

●接続エラー2（自動確認停止、相手先への接続のあと認証に失敗しました）

→ 相手先へ一度接続されましたが、リモートアクセス時の認証エラーなどで切断されました。以降、メールの自動確認は行われません。

→ ［メール設定（メール着信通知設定)］画面の［接続する相手先］で設定している相手先で、［送信ユーザID］［送信パスワード］などが正しく設定されているかどうか確認してください（[接続／相手先登録］画面参照)。

→ 相手先のリモートアクセスサーバの設定が正しいかどうか確認してください。

●POPエラー1（メールサーバ　ビジー）

→ メール（POP）サーバがビジーで、メール着信通知機能が正常に働きませんでした。以降も、メールの自動確認は継続して行われます。

●POPエラー2（自動確認停止、メールサーバ　ビジー）

→ 連続3回「POPエラー1（メールサーバ　ビジー)」が発生しました。以降、メールの自動確認は行われません。

→ しばらく待ってから再発信してください。

●POPエラー2（自動確認停止、メールアカウント、パスワード、認証方式を確認してください）

→ メール（POP）サーバで認証に失敗しました。以降、メールの自動確認は行われません。

→ ［メール設定（メール着信通知設定)］画面の［メールアカウント］［メールパスワード］［ユーザ認証］が正しく設定されているかどうか確認してください。

●POPエラー2（自動確認停止、POPコマンドエラー）

→ 設定の間違いやネットワークの問題などでPOPコマンドが正常にやり取りできませんでした。以降、メールの自動確認は行われません。

→ しばらく待ってから再発信してください。

→ パソコンからメールソフトなどを使って、ネットワークやメール（POP）サーバが正しく動作しているかどうか確認してください。

●POPエラー2（自動確認停止、POPコマンドがタイムアウトしました）

→ ネットワークやメール（POP）サーバの問題でPOPコマンドに対する応答を受け取ることができませんでした。以降、メールの自動確認は行われません。

→ しばらく待ってから再発信してください。

→ パソコンからメールソフトなどを使って、ネットワークやメール（POP）サーバが正しく動作しているかどうか確認してください。

●POPエラー2（自動確認停止、POPサーバがAPOP認証に対応していません）

→ メール（POP）サーバがAPOPの認証方式に対応していないため、認証に失敗しました。以降、メールの自動確認は行われません。

→ メール（POP）サーバがAPOPの認証方式に対応しているかどうか確認してください。

→ メール（POP）サーバがAPOPの認証方式に対応していないときは、[メール設定（メール着信通知設定）] 画面の [ユーザ認証] を [標準（POP3）] に設定してください。

●POPエラー2（自動確認停止、POP3サーバからタイムスタンプを取得できません）

→ メール（POP）サーバから送信されたタイムスタンプが長すぎるため、取得できませんでした。以降、メールの自動確認は行われません。

→ [メール設定（メール着信通知設定）] 画面の [メール（POP）サーバ] が正しく設定されているかどうか確認してください。

→ メール（POP）サーバがAPOPの認証方式に対応していないときは、[メール設定（メール着信通知設定）] 画面の [ユーザ認証] を [標準（POP3）] に設定してください。

●TCPエラー2（自動確認停止、サーバ名をIPアドレスに変換できませんでした）

→ ネットワークやメール（POP）サーバの設定の間違いなどで、名前で設定した [メール（POP）サーバ] をIPアドレスに変換できませんでした。以降、メールの自動確認は行われません。

→ ［メール設定（メール着信通知設定）］画面の［メール（POP）サーバ］が正しく設定されているかどうか確認してください。

→ DNSなどが正しく設定されているかどうか確認してください（［ルータ設定（LAN）］画面参照）。

→ 相手先に接続したときに、正しい経路情報が本製品に設定されているかどうかを確認してください（［IP経路］画面参照）。

●TCPエラー2（自動確認停止、メールサーバに接続できませんでした）

→ ネットワークやメール（POP）サーバの設定の間違いなどで、メール（POP）サーバにアクセスできませんでした。以降、メールの自動確認は行われません。

→ ［メール設定（メール着信通知設定）］画面の［メール（POP）サーバ］が正しく設定されているかどうか確認してください。

→ 相手先に接続したときに、正しい経路情報が本製品に設定されているかどうか確認してください（［IP経路］画面参照）。

3 クイック設定で自動的に設定されるフィルタ

クイック設定で、接続の設定を行うと［ルータ設定（LAN）］画面のオプション欄に次のフィルタが自動的に設定されます。
※フィルタ番号は異なる場合があります。

［ブロードバンドで設定］→［PPPoE端末型］

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「remote 1」のフィルタは「メイン（予備）：接続相手先登録#1」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2～#7）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#57によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#58によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録してください。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 43 reject in 10.0.0.0/8 * * * * remote 0
ip filter 44 reject in 172.16.0.0/12 * * * * remote 0
ip filter 45 reject in 192.168.0.0/16 * * * * remote 0
ip filter 46 reject in 10.0.0.0/8 * * * * remote 1
ip filter 47 reject in 172.16.0.0/12 * * * * remote 1
ip filter 48 reject in 192.168.0.0/16 * * * * remote 1
ip filter 49 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ送るのを防止するフィルタ

ip filter 47 reject out * 10.0.0.0/8 * * * remote 0
ip filter 48 reject out * 172.16.0.0/12 * * * remote 0
ip filter 49 reject out * 192.168.0.0/16 * * * remote 0
ip filter 53 reject out * 10.0.0.0/8 * * * remote 1
ip filter 54 reject out * 172.16.0.0/12 * * * remote 1
ip filter 55 reject out * 192.168.0.0/16 * * * remote 1
ip filter 57 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#47、#48、#53、#54は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、ま

たは必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直してください。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 *wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

［ブロードバンドで設定］→［PPPoE LAN型］

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2〜#7）を設定した場合は、「wanany」のフィルタのみ適用されます。
※「メイン（予備）：接続相手先登録#1」を設定すると「remote 1」のフィルタが追加されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 63 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 64 reject in * * tcpest * * wanany

フィルタ#63によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（‘ pass in ’）を登録してください。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 45 reject in 10.0.0.0/8 * * * * remote 0
ip filter 46 reject in 172.16.0.0/12 * * * * remote 0
ip filter 47 reject in 192.168.0.0/16 * * * * remote 0
ip filter 48 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ出るのを防止するフィルタ

ip filter 49 reject out * 10.0.0.0/8 * * * remote 0
ip filter 50 reject out * 172.16.0.0/12 * * * remote 0
ip filter 51 reject out * 192.168.0.0/16 * * * remote 0
ip filter 52 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 53 reject out * 169.254.0.0/16 * * * wanany

フィルタ#49、#50は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、または必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直してください。

● RIPのDirected-Broadcastに関するフィルタ

ip filter 59 pass in * 〈本体の属するネットワークアドレス〉/32 udp route route remote 0 nolog
ip filter 60 pass in * 〈本体の属するブロードキャストアドレス〉/32 udp route route remote 0 nolog
ip filter 61 reject in * 〈本体の属するネットワークアドレス〉/32 * * * remote 0
ip filter 62 reject in * 〈本体の属するブロードキャストアドレス〉/32 * * * remote 0

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 54 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 55 restrict out * * tcpfin * * wanany
ip filter 56 restrict out * * * * 137-139 wanany
ip filter 57 restrict out * * * 137-139 * wanany
ip filter 58 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ブロードバンドで接続] → [DHCP] / [Static]

● WAN(Ethernet)側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany
フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ(' pass in ')を登録してください。

● WAN(Ethernet)側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 49 reject in 10.0.0.0/8 * * * * wanether
ip filter 50 reject in 172.16.0.0/12 * * * * wanether
ip filter 51 reject in 192.168.0.0/16 * * * * wanether
ip filter 52 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスが不正なパケットがWAN(Ethernet)側へ出るのを防止するフィルタ

ip filter 53 reject out * 10.0.0.0/8 * * * wanether
ip filter 54 reject out * 172.16.0.0/12 * * * wanether
ip filter 55 reject out * 192.168.0.0/16 * * * wanether
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany
フィルタ#53、#54は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、または必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定しなおしてください。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ(工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。)

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ(工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。)

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ISDNで接続] → [端末型ダイヤルアップ]

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany
フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（‘pass in’）を登録してください。

● WAN側からの送信元IPアドレスが不正なパケットを破棄するためのフィルタ

ip filter 49 reject in 10.0.0.0/8 * * * * remote 0
ip filter 50 reject in 172.16.0.0/12 * * * * remote 0
ip filter 51 reject in 192.168.0.0/16 * * * * remote 0
ip filter 52 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN側へ出るのを防止するためのフィルタ

ip filter 53 reject out * 10.0.0.0/8 * * * remote 0
ip filter 54 reject out * 172.16.0.0/12 * * * remote 0
ip filter 55 reject out * 192.168.0.0/16 * * * remote 0
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#53、#54は、本体に設定されているIPアドレスがグローバルIPアドレスの場合のみ設定されます。本体をリモートアクセスサーバとして使用する場合は、このフィルタを削除するか、必要なフィルタを追加してください。フィルタが設定された後に本体のIPアドレスを変更した場合は、新しいIPアドレスに合わせてフィルタを設定し直してください。

● LAN上にWindows 2000 Serverがあるときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 60 reject dns qtype 6

● Webブラウザを終了するときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 61 restrict out * * tcpfin * * wanany
※「tcpfin」は、TCPセッションの終了（FIN）パケットおよびリセット（RST）パケットを対象とします。

● Windows XP/2000/98 SE/Meが行う定期的な通信によって起こる「意図しない自動接続」を防止するためのフィルタ：

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

[ISDNで接続] → [フレッツ・ISDN]

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「remote 1」のフィルタは「メイン（予備）：接続相手先登録#1」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2～#7）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録してください。

● WAN側からの送信元IPアドレスが不正なパケットを破棄するためのフィルタ

ip filter 43 reject in 10.0.0.0/8 * * * * remote 0
ip filter 44 reject in 172.16.0.0/12 * * * * remote 0
ip filter 45 reject in 192.168.0.0/16 * * * * remote 0
ip filter 46 reject in 10.0.0.0/8 * * * * remote 1
ip filter 47 reject in 172.16.0.0/12 * * * * remote 1
ip filter 48 reject in 192.168.0.0/16 * * * * remote 1
ip filter 49 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN側へ出るのを防止するためのフィルタ

ip filter 50 reject out * 10.0.0.0/8 * * * remote 0
ip filter 51 reject out * 172.16.0.0/12 * * * remote 0
ip filter 52 reject out * 192.168.0.0/16 * * * remote 0
ip filter 53 reject out * 10.0.0.0/8 * * * remote 1
ip filter 54 reject out * 172.16.0.0/12 * * * remote 1
ip filter 55 reject out * 192.168.0.0/16 * * * remote 1
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#50、#51、#53、#54は、本体に設定されているIPアドレスがグローバルIPアドレスの場合のみ設定されます。本体をリモートアクセスサーバとして使用する場合は、このフィルタを削除するか、必要に応じてフィルタを追加してください。
フィルタが設定された後に本体のIPアドレスを変更した場合は、新しいIPアドレスに合わせてフィルタを設定し直してください。

● LAN上にWindows2000 Serverがあるときに起こる「意図しない自動接続」を防止するためのフィルタ：

ip filter 60 reject dns qtype 6

● Webブラウザを終了するときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 61 restrict out * * tcpfin * * wanany

※「tcpfin」は、TCPセッションの終了（FIN）パケットおよびリセット（RST）パケットを対象とします。

● Windows XP/2000/98 SE/Meが行う定期的な通信によって起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

これらのフィルタによって、相手先の共有フォルダを利用する際に、Microsoftネットワークを利用できなくなることがあります。必要に応じて削除してください。
※フィルタ番号は異なる場合があります。

4 お問い合わせ先

メンテナンスサービスについて

- 本製品に含まれるソフトウェアが保存されている媒体に欠陥があった場合、お買い上げの販売代理店または小売店に返却してください。無償にて新品と交換いたします。なお、欠陥品送付にともなう送料は、送り主負担とさせていただきます。
- 本製品に含まれるハードウェアが購入後、１年間に通常のご使用において故障した場合、これを保証します。故障品に保証書を添えて、お買い上げの販売代理店または小売店に返却してください。無償にて修理いたします。なお、修理品送付にともなう送料は、送り主負担とさせていただきます。
- 保証期間でも次のような場合には、有償修理になります。
  (1) 保証書のご提示がない場合
  (2) 保証書に機器の製造番号、ご購入日、販売店名の記入がない場合、または字句を書き替えられた場合
  (3) 接続しているほかの機器に起因して生じた故障、または不当な修理や改造、調整をされた場合
  (4) 使用上の誤り、または故意・他意に関わらず、ほかの要因による損傷および故障の場合
  (5) 火災、地震、風水害、落雷、そのほかの天災地変、公害や異常電圧による損傷および故障の場合
  (6) 購入後の輸送、移動時の落下など、お取り扱いが不適当なため生じた損傷および故障の場合
  (7) 購入後の取り付け場所の移動、落下などにより生じた損傷および故障の場合

お問い合わせ先

本製品について技術的なご質問、または製品アップグレードに関するご質問は、お買い上げの販売代理店、小売店、またはMNテクニカルセンタまでお問い合わせください。

MNテクニカルセンタ

TEL： 0570−055−128（NTT 一般電話、携帯電話用）
　　　03−5550−8420（PHS、およびNTT以外の電話用）
FAX： 0570−056−128

※9:40〜17:50（土・日・休日・年末年始は除く）
※FAXは24時間受け付けております。

ホームページのご案内

株式会社エヌ・ティ・ティ エムイーのホームページにて、製品のサポート情報、マニュアル、最新のファームウェア、アプリケーションなどを提供する予定ですので、ご活用ください。

・株式会社エヌ・ティ・ティ エムイー「MN128 Information」
http://www.ntt-me.co.jp/mn128/

ADSL（Asymmetric Digital Subscriber Line）

上り方向と下り方向の通信速度が非対称な高速データ通信技術です。すでに一般家庭に普及している電話線を使って、インターネットへの高速で安価な常時接続環境を提供します。

APOP（Authenticated Post Office Protocol）

POPを利用してメールサーバ（POPサーバ）に接続する際に、使用するパスワードを毎回暗号化してユーザを認証する方法です。パスワードをそのまま送信するPOPより、セキュリティの高い方法といえます。

BACP（Bandwidth Allocation Control Protocol）

複数のチャネルを用いたMP通信で、リンクするチャネル数を制御するプロトコルです。MPで通信中にスループットBOD機能を用いて使用するチャネル数を自動的に変更するとき、チャネル数を変更してもよいかを接続先に問い合わせたり、接続先からチャネル数の変更を要求された場合に変更を許可するかどうかを接続先に知らせます。
BACPのプロトコル自体は、接続時にBACPに対応しているかどうかの確認だけに使用されます。実際に、使用するチャネル数の変更を接続先に要求したり、接続先からの要求に答える場合は、BAP（Bandwidth Allocation Protocol）が使用されます。

BAP（Bandwidth Allocation Protocol）

MPで通信中にスループットBOD機能を用いて使用するチャネル数を自動的に変換するとき、実際に接続先に使用するチャネル数の変更を要求したり、接続先から受けた要求に答えるプロトコルです。

BOOTP（Bootstrap Protocol）

TCP/IPネットワークにおいて、クライアントがシステムの起動に必要なプログラムをサーバから自動的に取得するプロトコルです。
BOOTPサーバは、ネットワークに関連した情報（IPアドレス、デフォルト・ルータのIPアドレス、設定ファイルのファイル名）などを管理しています。BOOTPクライアントが起動すると、BOOTPサーバが自動的にIPアドレスを割り振ります。
BOOTPサーバはクライアントとIPアドレスを一元的に管理しています（１つのクライアントに１つのIPアドレスが対応）。そのため、割り当てることができるIPアドレスの数とクライアントの数を等しくする必要があります。
本製品のDHCP/BOOTPサーバ機能を使う場合、BOOTPサーバだけをサポートしているMacintoshのMacTCPでは、IPアドレスだけが割り当てられます。

CHAP（Challenge Handshake Authentication Protocol）

PPP接続で使用されるユーザ認証方法の１つです。最初にPPPサーバがChallenge Valueという乱数をPPPクライアントに送ります。PPPクライアントはその乱数を使ってパスワードを演算し、その結果をPPPサーバに返します。PPPサーバは受け取った値と自分で計算した値とを比較し、同じであれば接続を許可します。
Challenge Valueは認証のたびに変えるため、同じユーザー名とパスワードでも演算の結果は毎回異なります。したがって、たとえ通信回線を盗聴されても、不正利用される可能性は低くなります。ユーザ名とパスワードだけで単純に認証するPAPよりセキュリティの高い方法といえます。

DHCP（Dynamic Host Configuration Protocol）

TCP/IPネットワークにおいて、クライアントがシステムの起動に必要なプログラムをサーバから自動的に取得するプロトコルです。DHCPはBOOTPを拡張したプロトコルです。
DHCPサーバは、ネットワークに関連した情報（IPアドレス、デフォルト・ルータのIPアドレス、設定ファイルのファイル名、ドメイン名）などを管理しています。DHCPクライアントが起動すると、DHCPサーバが自動的にIPアドレスを割り振ります。
DHCPクライアントに割り当てるIPアドレスの有効期限を設定できます。有効期限を過ぎると割り当て済みのIPアドレスを再利用することができるので、効率よくIPアドレスを使用することができます。
本製品のDHCP/BOOTPサーバ機能を使う場合、DHCPサーバをサポートしているTCP/IPでは、IPアドレスのほかにデフォルト・ルータのIPアドレスなどが割り当てられます。

DHCP/BOOTPサーバ機能

→活用ガイド～中・上級編「技術解説」

DNS（Domain Name System）

TCP/IPネットワークにおける名前解決サービスのことです。DNS（ドメイン・ネーム・システム）にしたがってドメインネームサーバにコンピュータ名やドメイン名を登録して、ドメインネームサービスを提供しています。ドメインネームサービスを利用すると、「192.168.0.1」などの分かりにくい数字ではなく、分かりやすいドメイン名やホスト名で目的のサイトを指定することができます。

DMZ（DeMilitarized Zone）
LAN側のネットワークとインターネットとの間に、ルータを介して設けられる区域のことです。
インターネットにWebサーバなどを公開することによってLAN型で接続している端末に、インターネットから不正な接続がされる可能性を減らすために、サーバをこの区域に設定します。

FTP（File Transfer Protocol）
TCP/IPネットワークでファイルを転送するためのプロトコル、またはそのサービスを指します。FTPはおもに、ホストから自分のコンピュータへのファイル転送に使われます。インターネット上に多数存在するFTPサーバから、フリーウェアやシェアウェア、サウンドや画像のデータをダウンロードしたり、自作のプログラムやデータをFTPサーバへアップロードして公開しています。

IP（Internet Protocol）
TCP/IPネットワークにおけるネットワーク層プロトコルです。ネットワーク内またはネットワーク間のデータパケット送受信を制御するコネクションレス型プロトコルです。

IPCP（Internet Protocol Control Protocol）
PPPは主に、LCPとNCP（Network Control Protocol）の2種類のプロトコルで構成されています。NCPは、ネットワーク層プロトコルをPPP環境で使用するための制御機能を実現します。NCPはネットワーク層プロトコルごとに規定する必要があり、IP用に規定されているのがIPCPです。クライアントへIPアドレスを割り当てたりします。

IP Masquerade
→活用ガイド～中・上級編「技術解説」

IPsec（Security Architecture for Internet Protocol）
→活用ガイド～中・上級編「技術解説」

IPフィルタ
→「フィルタ」

L2TP（Layer2 Tunneling Protocol）
→活用ガイド～中・上級編「技術解説」

LAN型ダイヤルアップ接続
LANとLANを電話回線を介して接続するための契約です。この契約をしたときは、LANの規模に応じたIPアドレスがプロバイダから指定され、そのIPアドレスを設定してプロバイダに接続します。

MACアドレス
ネットワーク上の個々の端末を区別するための物理アドレスです。すべてのEthernetカードには固有のアドレスが割り当てられていて、これを元にデータの送受信が行われます。アドレスはIEEE（アメリカ電気電子学会）によって世界的に管理されています。
MACアドレスの確認方法は、活用ガイド～中・上級編「パソコンのMACアドレスを確認する」を参照してください。

MP（PPP Multilink Protocol）
ISDN回線で高速通信を実現する方法の１つで、複数のチャネルを使用してPPP通信する方式のことです。INSネット64の2つのBチャネルを同時に接続すると、128kbpsの通信速度が可能になります。

MPPE（Microsoft Point to Point Encryption）
PPPでのダイヤルアップ接続、またはPPTP VPN接続のデータを暗号化する方法で、本製品ではMPPEでは暗号化アルゴリズムとしてRC4を使用し、鍵長は40bitと128bitをサポートしています。なお、MPPEには、MS-CHAPによって生成された共通のクライアントキーとサーバキーが必要です。

MSS（Maximum Segment Size）
TCP接続をする際に、1つのTCPパケットとして受信できるデータサイズの最大値を、相手先に通知するためのTCPのオプションです。

MTU（Max Transfer Unit）
TCP/IPのパケットサイズの最大値を決めるパラメータのことです。

OCN（Open Computer Network）
NTTが提供するデータ通信用の回線サービスのことです。インターネットで使用されているTCP/IPを基調にしていて、インターネットにも接続されています。OCNのサービスには、インターネットへ常時接続する「OCN常時接続サービス」と、必要なときに電話をかけて接続する「OCNダイヤルアクセスサービス」があります。

OCNエコノミーサービス
OCN常時接続サービスのうち、もっとも低料金のサービスです。OCNエコノミーサービスを契約すると、アクセス時間や電話料金を気にせず、インターネットを利用できます。本製品では、OCN常時接続サービスのうち、このOCNエコノミーサービスのみ使用できます。

PPTP（Point to Point Tunneling Protocol）
→活用ガイド～中・上級編「技術解説」

Super G
米アセロス・コミュニケーションズ社の開発した、無線欄のスループットを向上させる技術です。同社の独自技術である、「パケットバースト転送」「動的な転送最適化」「データ圧縮機能」を組み合わせることで、実効スループットを大幅に向上しています。

UPnP（Universal Plug and Play）
インターネットで標準になっている技術を元にして、家庭内にあるパソコンやAV機器、電話、家電製品などをネットワークにつなぐだけで利用可能にすることを目指した技術です。本製品はこの技術に対応しており、同じくUPnPに対応したアプリケーションソフトである「Windows Messenger」や「MSN Messenger」を利用して、複雑な設定なしにインターネット上での通話を行うことができます。

VPN（Virtual Private Network）
→活用ガイド～中・上級編「技術解説」

WINS（Windows Internet Name Service）
Windowsのコンピュータ名とIPアドレスを結びつける名前解決サービスの１つです。WINSクライアントは起動するとWINSサーバにコンピュータ名とIPアドレスを登録し、WINSサーバは定期的に各サブネットのコンピュータ名とIPアドレスの情報を交換します。WINSクライアントは、WINSサーバからサブネットをまたがる他のWINSクライアントのコンピュータ名とIPアドレスの情報を取得することができます。

WEP（Wired Equivalent Privacy）
無線LANの国際規格のIEEE802.11で決められている暗号化技術です。アクセスポイントと端末の両方で、同じ文字列からなる「キー（鍵）」を設定しておき、そのキーを使ってデータの暗号化や復号化が行われます。

WPA-PSK
WPA（Wi-Fi Protected Access）とは、Wi-Fi Allianceが提唱する認証と暗号化をあわせた最新のセキュリティ規格です。本製品では、Pre-Shared Key（WPA共有キー）を利用する「WPA-PSKモード」が利用できます。従来から利用されているWEPの弱点を克服した暗号化方式「TKIP」や、次世代の標準と言われる強力な暗号化方式「AES」を利用できるので、無線LANのセキュリティ強度を大幅に向上させることができます。

アクセスポイント
無線LANカードを装着したパソコンと有線LANの通信を中継したり、無線LANカードを装着したパソコン同士の通信を中継する機器のことです。

グローバル着信
INSネット64でダイヤルインサービスを使用しているときに、契約者回線番号側への着番号の通知を省略するどうかを指定する機能です。INSネット64の契約時に「グローバル着信あり」にすると、相手側から契約者回線番号で着信要求があったとき、通信できるすべての機器が着信します。このとき、本製品でグローバル着信の設定を行うと、特定の機器にのみ着信させることが可能になります。

サブネットアドレス通知サービス
INSネット64の基本サービスの1つです。使用しているISDN回線に複数のISDN機器がつながっている場合に、それぞれの機器にサブアドレスを付けることができます。このサービスを利用すると、相手がこちらに接続するときに、回線番号に加えてサブアドレスを指定することにより、特定の機器を直接指定することができるようになります。

サブネット/サブネットマスク
32ビットで構成されるIPアドレスは、クラスに応じてネットワーク番号とホスト番号に分けられます。ネットワーク番号は、固有のネットワークに割り当てられ、各ホストにはホスト番号を割り当てます。このとき、サブネットマスクを指定すると、ネットワークの中でさらにサブネットを指定することができ、ネットワーク構築の自由度が上がります。サブネットマスクは、32ビットのうちサブネットとして指定したい部分を1で表し、「11111111.11111111.11111111.00000000」などのように設定しますが、通常10進数で「255.255.255.0」のように表します。

スイッチングハブ
パソコンなどの端末から送られてきたデータをMACアドレスをベースに解析し、送り先の端末だけにデータを送信する機能を搭載しているハブのことです。

スタティックルーティング
ユーザがあらかじめ中継経路（ルーティングテーブル）を固定的に設定する方式のことです。

スタティックルート
ユーザがあらかじめ決めた中継経路のことです。

ステートフル・パケット・インスペクション

（SPI）
ファイヤーウォールを通過するパケットのデータを読み取って内容を判断し、動的にポートを開放したり閉鎖したりする機能です。

ステルスモード
インターネット側から送信されるPingコマンド（ポート打診）に応答せず、またICMPエラーやTCPリセットを返さなくなる機能です。外部からの不正侵入のために行われることもある外部からのポートスキャンに反応しないので、インターネット上で本製品の存在を隠すことができます。

セッション
ネットワーク上の2つのホスト間の通信のことです。個々のホストは、同時に複数のセッションを行うことができます。

ダイナミックルーティング
ルータ同士で経路情報やトラフィック情報をやりとりすることによって、中継するルータの数や遅延時間が最小になる最適な経路を自動的に選択して、パケットを転送する方式のことです。

端末型ダイヤルアップ
１台のパソコンでインターネットを利用するための契約です。この契約をしたときはプロバイダに接続したときに、そのパソコンのIPアドレスが割り当てられます。
ただし、本製品ではLANにつながっているパソコンでも端末型ダイヤルアップ接続の契約でインターネットを利用できます。

デフォルトルータアドレス
→活用ガイド～中・上級編「技術解説」

デフォルトルート
パケットを送信するときに、そのアドレスがルーティングテーブル内に明示的に記載されていないときに使用される、デフォルトルータまでの経路のことです。

ドメイン名
インターネットに接続するコンピュータはIPアドレスと呼ばれる数字を使って識別されていますが、数字よりも簡単に覚えられるように考えられた文字で表現された名前のことです。
ドメイン名は、文字の並びであるラベル、あるいはピリオドで区切られた複数のラベルから構成されます。
例）株式会社エヌ・ティ・ティ エムイーのドメイン名
　　ntt-me.co.jp
上記の場合、ntt-me、co、jpの3つのラベルがあり、ドメイン名としてはntt-me.co.jp、co.jp、jpの3つのレベルのドメインから構成されます。

ドメイン名解決要求／解決応答
DNS（ドメインネームシステム）サーバには、ドメイン名と対応するIPアドレスが登録されています。通信したい相手のIPアドレスがわからない場合、DNSサーバにドメイン名を問い合わせると、そのドメイン名に対応するIPアドレスが通知されます。

ニーモニック
複雑な情報や長い情報を、簡単で覚えやすいものと結びつけるのに使用される単語など、記憶の助けになるものを指します。

パケット
ネットワーク上を流れるデータの単位で、制御信号からなるヘッダと情報データを含むビット列のことです。ヘッダには宛先アドレスや送信元アドレス、データの内容を表わすフラグなどが記録されており、プロトコルや通信方法によって多様です。

ハブ
LANを拡大するためのハードウェアです。ハブには複数のポートがついていて、各ポートにパソコン、ワークステーション、サーバなどを接続できます。
ハブにルーティング、ネットワーク管理などの機能が追加され、ネットワークの中心となっているものもあります。
LANを構築する場合、10/100BASE-Tケーブルを使用するときは、ハブが必要になります。

ファイアウォール
内部のネットワークへ、外部から侵入されることを防ぐシステムです。内部のネットワークと外部のネットワークの境界でデータを監視し、不正なアクセスを検出したり遮断したりします。このシステムが組み込まれたコンピュータ自身をさして「ファィアウォール」と呼ぶこともあります。

フィルタ
通過しようとするデータになんらかの処理を施すものです。アドレスを元に、通すパケットと通さないパケットを判別するために使用します。

フィルタリング
通すべきでないデータを遮断することです。
トラフィックの増大を防いだり、不正なアクセスを防いだりします。

ブロードキャスト
同一のネットワーク内のすべてのハードウェアへパ

ケットを送信すること（同報通信）です。

ブロードキャストアドレス

→活用ガイド～中・上級編「技術解説」

ブロードバンド

xDSL、CATV、光ファイバーなど、帯域幅が広く転送能力が高い通信方式の総称です。

ホスト

インターネットでは、WWWサーバやメールサーバなどの各種サービスを行うコンピュータをホストとして扱います。

ポート番号

通信を行うアプリケーションとTCPまたはUDPを対応付ける番号のことです。

ホップカウント

パケットが伝送されている間に通ったルータの数を指します。RIPではホップカウントを16に制限しています。

リセット（RST）パケット

このパケットは、再送信などの通常の方法で回復できないエラーが発生した場合や、サーバがシステムダウンした場合に使われます。

リモートアクセス

公衆電話回線などを使用して、遠隔地のパソコンからLANなどのネットワークに接続することです。LANにリモートアクセスすると、LANに直接つながっているパソコンと同様に、データ共有、プリンタ共有などLANの資源を使用することができます。

リモートアクセスIPクライアント

PPPソフトを使用して、遠隔地のパソコンから電話回線を介してTCP/IPのLANに接続するユーザのことを指します。

索引

英数字

IPアドレス 96
MAILランプ....60
Messenger 75
MP 14
MSS 5
MTU 6
NTPサーバ....81
OCNエコノミー接続....19
PPPoE 4
UPnPポート....77

あ

アップデータ 102
インターネット接続
　ISDN ....14、17、19
　ブロードバンド....4
エラー一覧....124

さ

再起動 105
最大接続時間 56
サポートセンタ....138
時刻設定 81
自動接続 26
自動接続制限
　状況....41
　時間帯による～....29、32
　接続回数による～....39
　通信料金による....36
自動切断 46
　タイマ ....49、53
セッションキープアライブ....8
接続
　自動....26
　手動....23
　設定 ....4、14、17
接続状況 86
接続／切断ログ....89
切断
　自動....46
　手動....44
設定
　書き込み 99
　確認....97
　初期状態 100
　保存....98
設定ページ
　ユーザID....7、84
　パスワード ....7、84

た

通信料金情報....92、95

は

バックアップ機能 11
バージョンアップ 102
パスワード ....7、84
ファームウェア ....101、102
ブロードバンド....4

ま

メール
　閲覧....69
　消去....71
　転送....72
　フィルタ 66
メール着信通知機能....57、60
　指定時間間隔 58
　指定時刻 62
　手動....65
　特定のメール 66

や

ユーザID....7、84

ら

リソースBOD....79